Wave

Global Administrator Guide

Release 4.0

June 2013

Vertical Communications, Inc. reserves the right to revise this publication and to make changes in content without notice.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY

Vertical Communications, Inc. makes no representation or warranties with respect to the accuracy or completeness of the content of this publication and specifically disclaims any implied warranty of merchantability or fitness for any particular purpose, and shall not be liable for any loss of profit or any other commercial damage, including but not limited to, special, incidental, or consequential.

TRADEMARKS

Vertical Communications and the Vertical Communications logo and combinations thereof and Wave Global Administrator, Wave ViewPoint, Wave IP 2500, Wave IP 500, Wave Fax Manager, Wave Service Response, and Wave Voice Server are trademarks of Vertical Communications, Inc. All other brand and product names are used for identification only and are the property of their respective holders.

What’s new in this version

NEW FOR THIS RELEASE

- **Wave OpenVPN Server** is now the preferred method to enhance remote phone integration. OpenVPN Server allows phones outside of your network to behave the same as local phones. See page 6-61.
- **NAT traversal** is now one method to enhance remote phone integration. NAT traversal requires:
  - Remote user configuration. See 6-37.
  - Wave Server configuration. See 6-64.
  - Router configuration. See *Configuring the SonicWALL TZ215 Router for NAT Traversal* or *Configuring the Cisco 881 Router for NAT Traversal*.
- Wave **MeetMe conferencing** expands Wave’s ad-hoc conferencing capability by providing support for up to 18 conference rooms, with up to 24 attendees per conference. See page 16-16.
- The new **Wave Phonebook is a searchable directory of public ViewPoint Groups or private contacts** that is accessible directly from a button on a user’s Edge 5000i IP phone. See page 11-86.
- **SIP paging is now supported** via Wave’s zone paging feature. Multicast SIP paging is the preferred method, although both multicast and unicast SIP paging are supported.. See page 16-39.
- **Secure Sockets Layer (SSL) is now supported** to provide standard e-mail notifications when you use a hosted service such as Microsoft Office365 or gmail as your company mail server. You configure this option via System Settings in User/Group Management.. See page 4-12.

- **You can now change SIP registration expiration timer default values** via SIP Advanced Parameters in IP Telephony.
  - Phone Registration Expiration
  - Inbound SCP Registration Expiration
  - Outbound SCP Registration Expiration

  You may need to change the default timer values to support some ITSPs. See page 6-9.
- Starting with Wave 4.0, **global SIP endpoint authentication will be enable on all new Wave Servers as a standard security measure**. Vertical strongly recommends that global SIP endpoint authentication be enabled on all existing Wave Servers. See page 6-11.
- **Propagate cut through call progress messages on tandem SIP trunks is now supported** as part of SCP configuration. This option may be required to support some ITSPs. See page 6-24.
- When you activate a license, you will now be asked if you want to participate in the **Vertical Product Usage Improvement Plan**. See page 24-1.

REVISED FOR THIS RELEASE

The following sections are updated:

- **“Setting up system-wide audio options”:** The Hold audio file volume slider control that appears on the System Settings Audio tab in User/Group Management is not supported in this version. See page 4-18.
- **“Modifying advanced SIP timers”:** Expanded descriptions of SIP Session timers in the SIP Advanced Parameters dialog in IP Telephony. See page 6-7.
- **“Changing the ViewPoint Mobile Port”:** When setting up ViewPoint Mobile, your firewall must allow outbound connectivity from the Wave Server on the port that you specify. See page 11-6.
- **“Configuring authorization codes”:** Removed obsolete note that authorization codes are not supported on SIP phones—authorization codes are supported on all phone types. See page 16-2.

- **“Setting up instant messaging permissions for users”:** Added Important note recommending that you IM permission if you have a large number of virtual users, to avoid negatively impacting system performance. See page 16-44.
- **“System resource types”:** Ad-Hoc Conference resources have been renamed All Conferencing resources, and are used for both ad-hoc conference requests and MeetMe conference rooms. See page 23-50.
- **“Wave Software License Agreement”:** This appendix has been removed from this manual. You now have the option to view the Vertical End User License Agreement (EULA) when you activate a Wave license. You must select the associated checkbox and accept the EULA to continue the license activation process.

The following sections were added:

- **“Joining the Wave Server to a Windows domain”:** See page 3-13.
- **“Using Windows Active Directory accounts to administer Wave”:** See page 3-14.

For details on everything that’s new in Wave 4.0, see the *Wave 4.0 Release Notes*.

Contents

Part 1 Initial Configuration and Administration

Chapter 1. About This Guide

Chapter Chapter 2Navigating the Management Console

Chapter 3. Before You Begin

Chapter 6 IP Telephony Configuration

Chapter 7. Initial Call Routing Configuration

Chapter 8. Configuring Inbound Call Routing

Chapter 9. Configuring Outbound Call Routing

Chapter 10. Configuring Phones

Chapter 11. Managing Users and Roles

Chapter 12. Managing ViewPoint Groups

Chapter 13. Configuring Auto Attendants

Chapter 14. Data Networking Configuration

Chapter 15. Initial System Administration

Chapter 17. Advanced Trunk and Channel Configuration

Chapter 18. Managing System Prompts and Audio

Chapter 19. Recording All Wave Calls

Chapter 20. Tracking and Distinguishing Calls

Chapter 21. Advanced Data Networking Configuration

Chapter 22. Monitoring and Maintenance

Chapter 23. Continuing System Administration

Chapter 25. Connecting Wave Servers via WaveNet

Chapter 26. Using the Call Classifier

Part 3 Key Wave Concepts

Chapter 27. Understanding Wave Trunks

Chapter 28. Understanding Wave IP Telephony

Part 4 Reference

Chapter 31. Wave Reports

Chapter 32. SNMP Agents

Part 1

Initial Configuration and Administration

Chapter 1

About This Guide

CHAPTER CONTENTS

About Wave ISM

Welcome to Wave ISM, a unified platform designed for scalability, reliability, and ease of use that delivers comprehensive communication support, including PBX voice capability, multiprotocol router capabilities, full LAN/WAN connectivity, and a suite of communication applications.

Getting the most out of this guide

This guide provides detailed information about configuring the Vertical Wave Server and Vertical Wave system software.

This guide is intended for network administrators, phone system administrators, and office personnel who are responsible for configuring and maintaining the Wave system.

This guide provides information about all parts of the remote administration interface used to perform the configuration and system administration steps to set up the Wave system. An extensive online Help system provides detailed information about additional functionality not described in this guide.

Note how the following terms are used in this guide:

- "**Wave ISM**" refers to the Wave software infrastructure, Wave Integrated Services Manager.
- "**Wave Server**" refers to the physical server PC on which Wave ISM runs. Most of the information in this guide applies to all Wave Server models. When information applies to a specific to a Wave Server model, the model is identified, for example "Wave IP 2500" or "Wave IP 500". For more about the different Wave Server models, see the *Wave Server Installation Guide*.
- "**Wave**" refers to your Wave phone system as a whole.

Where to start

This guide includes information for readers at a variety of levels. To get the most out of the documentation, start by reading the parts that are most relevant to your level of experience.

For new Wave system administrators

1. Begin by reading Part 3, "Key Wave Concepts"
2. Next, work through the procedures in Part 1, "Initial Configuration and Administration" to configure the basic Wave system settings.
3. Then choose the advanced features you wish to configure from Part 2, "Advanced Configuration and Administration".
4. Refer to Part 4, "Reference", as necessary.

That's all you need to begin configuring most typical Wave system installations.

For experienced Wave system administrators

1. Begin by working through the procedures in Part 1, “Initial Configuration and Administration”, to configure the basic Wave ISM system settings.
2. Then choose the advanced features you wish to configure from Part 2, “Advanced Configuration and Administration”.
3. Refer to Part 3, “Key Wave Concepts”, and Part 4, “Reference”, as necessary.

Using the Help system

The Wave Help system provides context-sensitive Help. To access Help, use the following methods:

- From the Wave Global Administrator Management Console, click the Help icon located at the top right corner, then select a topic from either the Contents tab or the Index tab. Use the Search tab to locate topics that include specific text.
- From each Management Console applet, click the Help button to directly access the relevant Help topic.

Conventions used in this guide

In the course of describing Wave system features and functions, this guide uses the conventions described in this section.

Special messages

Note: A note highlights information that is important or of special interest.

Hint: A hint relays information to help you perform a task.

Caution! *A caution highlights information that helps you prevent damage to the equipment or to data. It tells you how to avoid the problem.*

Warning! *A warning alerts you to a situation that could cause you physical harm.*

Type conventions

Type Convention	Used to Indicate
Bold	User interface elements (buttons, field labels, and tab labels)
Italics	Book titles, glossary words, and word emphasis
`Courier font`	Screen text and user-typed command line entries
Initial Caps	Product names, menu titles, window titles, application titles, dialog titles, hypertext links, file names, and directories

Terms used

Term	How to Interact
Click	Click the left mouse button.
Right-click	Click the right mouse button.
Shift-click	Hold the Shift key while clicking the left mouse button.
Ctrl-click	Hold the Ctrl key while clicking the left mouse button.
Ctrl+Q	Hold the Ctrl key while pressing one or more additional keys.
Enter	Press the Enter key or select OK.
Type	Type the indicated text, but *do not* press the Enter key or select OK.
Press	Press only the key or keys referred to.
Check	Place a check mark in the check box.
Select	Choose an option from a menu, drop-down list, or list of radio buttons.

Related reading

For information about this version of Wave ISM, including new features, known issues, and other late-breaking information, see the Release Notes included on the Documentation CD.

The following additional documents are included with the Wave Server in Acrobat format, and can be found on the Documentation CD.

Manuals

Wave Server Installation Guide. Provides detailed instructions for physically installing the Wave Server and Wave ISM and performing initial system configuration.

Wave ISM System Recovery Guide. Describes how to use the Wave ISM System Recovery Disk to restore your Wave Server to its original factory settings for emergency recovery.

Wave ViewPoint User Guide. Provides task-based instructions on how to use ViewPoint, including call control, working from remote locations, participating as an agent in a Contact Center, and so forth.

Wave Phone User Guide. Describes how to use SIP phones, digital phones, analog phones, and SIUP softphones with Wave.

Wave Server Hardware Reference Guide. Provides detailed technical information about the Wave Server hardware components.

Wave Contact Center Administrator Guide. Describes how to use the separately-licensed Wave Contact Center to provide full-featured call distribution.

Quick Reference Guides

Wave Analog Phone Quick Reference Guide. Provides instructions for using analog phones with Wave.

Wave Digital Phone Quick Reference Guide. Provides instructions for digital phones with Wave.

Wave SIP Phone Quick Reference Guide. Provides instructions for using SIP phones with Wave.

Wave Voice Mail Quick Reference Guide. Provides instructions for using Wave ISM Voice Mail features.

Support services

Vertical Communications has worked diligently to produce the highest quality communications system possible. In the course of installing or customizing a system customers may require personal attention.

For technical support contact your Vertical Wave provider.

Web site

For more information about Vertical Communications, Inc. and the Vertical Wave product line, contact your Vertical Wave provider. To do so, call 1-877-VERTICAL, or visit the Vertical corporate Web site:

```
http://www.vertical.com
```

System security

You are responsible for the security of your Wave system. Unauthorized use of the Wave system could result in toll fraud. Your system administrator must read all system administration documentation to understand which configuration options can introduce the risk of toll fraud and which configuration options can be activated or deactivated to prevent it.

For more information, see Appendix A, “Protecting Your Phone System Against Toll Fraud.”

Note: Vertical Communications, Inc. does not warrant that the configuration software is immune from or will prevent unauthorized use of common-carrier telecommunications facilities and services accessed through or connected to the Wave Server. Vertical Communications, Inc. is not responsible for any charges resulting from unauthorized use.

Chapter 2

Navigating the Management Console

Chapter Contents

This chapter describes how to log on and use the Global Administrator Management Console

Before logging on

Verify that the Wave Server has been added to the Internet Explorer Local Intranet group.

Note: This step may have been performed during system installation, as described in “Connecting to the Wave Server via your network” in Chapter 5 in the *Wave Server Installation Guide*.

To add the Wave Server to the Internet Explorer Local Intranet group

1. In Internet Explorer, choose **Tools > Internet Options.**
2. On the Security tab, click **Local intranet** in the **Select a zone...** box, and then click **Sites**.
3. In the Local Intranet dialog, click **Advanced**.
4. If the Wave Server does not appear in the **Websites** list, in the **Add this website to the zone** text box, enter the the default IP address of the Vertical Application Module (VAM) in the Wave Server (192.168.205.1), or the VAM's IP address on your system if you have changed it). You do not need to preface the IP address with http:// or ftp://.
5. Click **Add** to add the new entry to the **Websites** list.
6. Click **Close**, and then click **OK** twice to close all dialogs.

Logging on for the first time

During installation, you connected an administrator PC to the Wave Server using a modem or an Ethernet port on the Integrated Services Card. If you have not yet made an initial connection, see Chapter 4 in the *Wave Server Installation Guide* for instructions.

The first time you log on to the Management Console, you use a default user name and password. You will change the default name and password later.

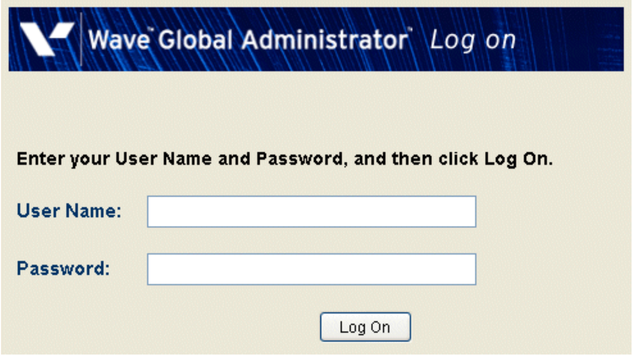
To log on for the first time

1. On the client workstation, launch Microsoft Internet Explorer.
2. Enter the default host name or IP address on the address line of your browser.

   The default host name is `io-default`. The default IP address is `192.168.205.1`.

   Note: When you launch the Management Console, a dialog may appear asking you to install a specific version of the Java 2 runtime environment (JRE). (This message will only appear if the version detected is less than the minimum version supported by Wave.) Click **Yes** to perform the installation.

The Wave Global Administrator Log On dialog opens.



Enter your User Name and Password, and then click Log On.

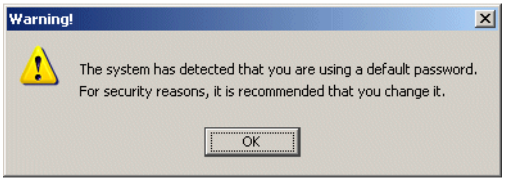
3 Enter your user name and password. The initial default logon values are:

User Name. `GlobalAdministrator`

Password. `Vertical4VoIP!`

Note: **Password** is case-sensitive.

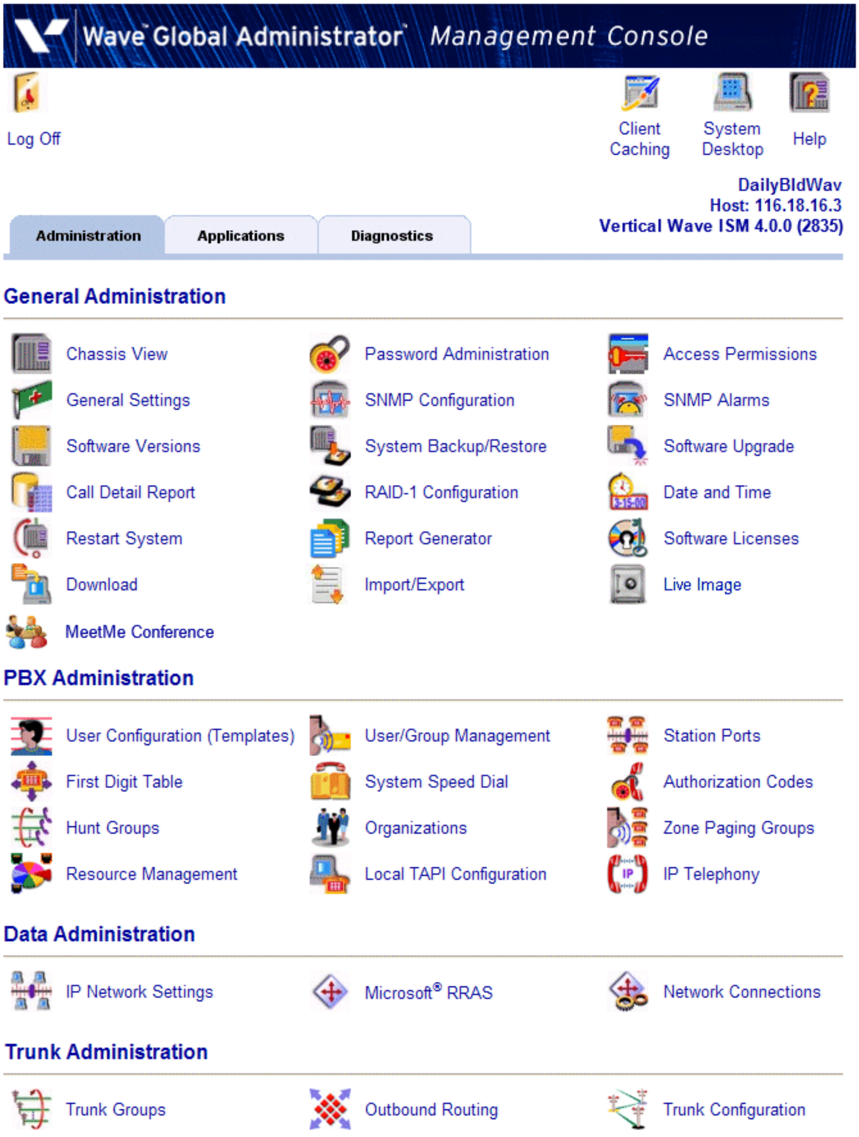
You will see the following warning each time you log on using the default password:



The system has detected that you are using a default password. For security reasons, it is recommended that you change it.

4 Click **Log On**. If other users are logged on to the Management Console, a list of logged on users will appear. Click **OK** to close the dialog.

If your logon is successful, the Management Console opens.



Wave Global Administrator Management Console

Log Off

Client Caching

System Desktop

Help

DailyBldWav
Host: 116.18.16.3
Vertical Wave ISM 4.0.0 (2835)

Administration | Applications | Diagnostics

General Administration

Chassis View	Password Administration	Access Permissions
General Settings	SNMP Configuration	SNMP Alarms
Software Versions	System Backup/Restore	Software Upgrade
Call Detail Report	RAID-1 Configuration	Date and Time
Restart System	Report Generator	Software Licenses
Download	Import/Export	Live Image
MeetMe Conference		

PBX Administration

User Configuration (Templates)	User/Group Management	Station Ports
First Digit Table	System Speed Dial	Authorization Codes
Hunt Groups	Organizations	Zone Paging Groups
Resource Management	Local TAPI Configuration	IP Telephony

Data Administration

IP Network Settings	Microsoft® RRAS	Network Connections

Trunk Administration

Trunk Groups	Outbound Routing	Trunk Configuration

Management Console basics

The Wave Global Administrator Management Console is a portal to the applets and their associated dialogs that are used to configure and manage Wave ISM.

More information is available about how to use an applet:

- **Administration tab applets**. See this manual, or click **Help** in an applet dialog.
- **Applications tab applets**. See the documentation for that application.
- **Diagnostics tab applet**. Click **Help** in an applet dialog.

This section describes:

- Starting and exiting applets. See page 2-5.
- Navigating applet tree structures. See page 2-11.

Note: If you are accessing the Management Console from an administrator PC running Microsoft Windows XP SP2 and you experience problems, for example applets appear to be disabled or hidden, see “Troubleshooting Management Console problems” in Appendix G in the *Wave Server Installation Guide*.

Starting and exiting applets

To start any applet, click its icon or name in the Management Console. Exiting an applet is slightly different depending on the applet type. See the following:

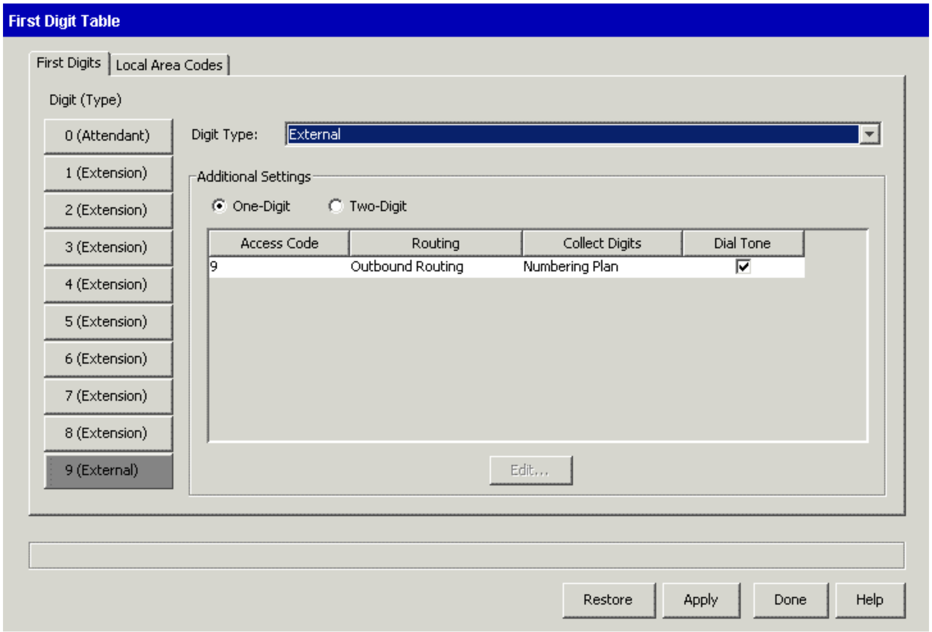
- Dialog applets vs. remote access applets
- Dialog applets
- Navigating applet tree structures

Dialog applets vs. remote access applets

There are two types of applets accessible from the Management Console, dialog applets and remote access applets.

Dialog applets

Most applets are dialog applets. Dialog applets directly open a master dialog, for example the First Digit Table applet:



First Digit Table

Digit Type: External

Additional Settings

● One-Digit ○ Two-Digit

Access Code	Routing	Collect Digits	Dial Tone
9	Outbound Routing	Numbering Plan	☑

Some applets consist of a single master dialog, while others may link to sub-dialogs.

Exiting a dialog applet

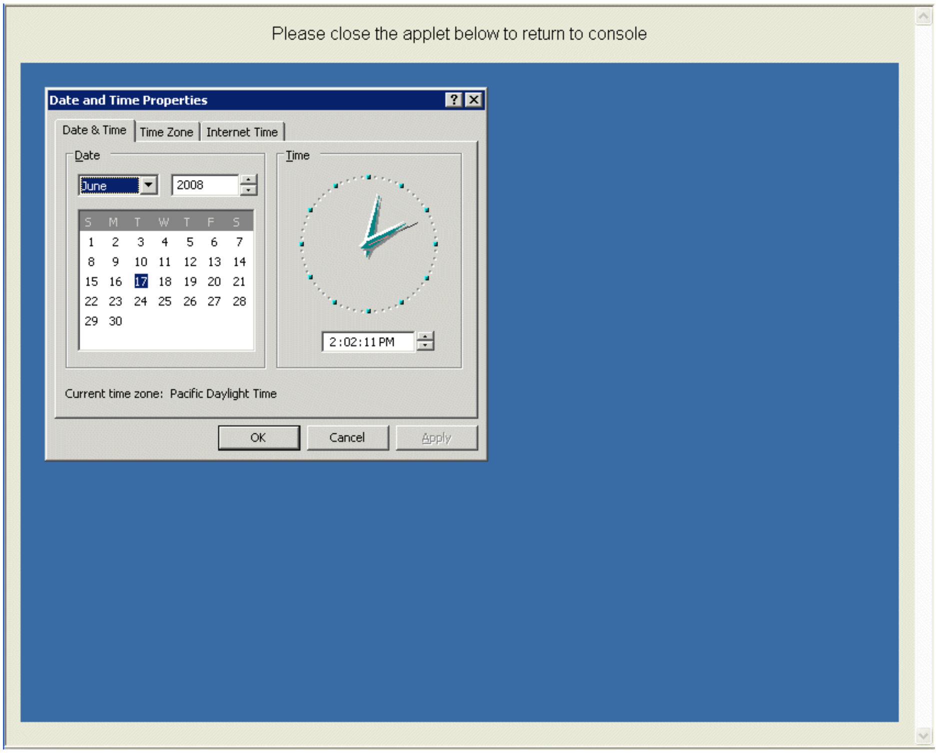
Click **Done** or **OK** to close each sub-dialog until you return to the master dialog.

From most master dialogs, you can click any of the following:

- **Done.** Exits the dialog, prompting you to save any changes that you made.
- **Restore.** Returns the fields in the dialog to the previous (unmodified) values.
- **Apply.** Saves your changes without closing the dialog.
- **Help.** Opens a Help topic that describes how to configure the settings in the master dialog and any associated sub-dialogs.

Remote access applets

Some Management Console applets (listed in the next table) open a Remote Desktop Connection to the associated application, for example the Date and Time applet:



Please close the applet below to return to console

Date: June 2008

Time: 2:02:11 PM

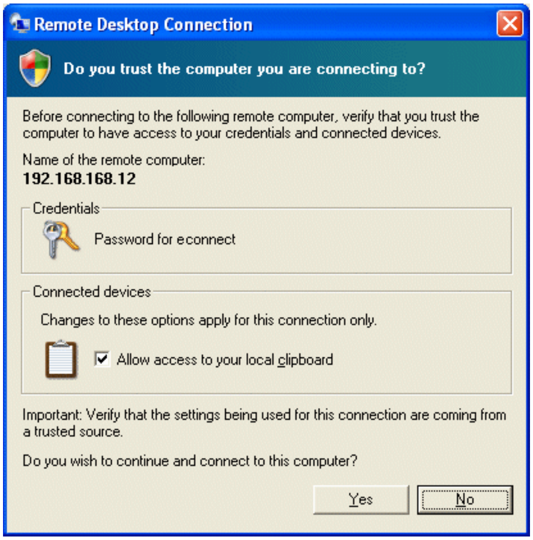
Current time zone: Pacific Daylight Time

The following table lists the Management Console applets that are launched through remote access:

Tab	Applet	For more information, see...
Administration	**RAID 1 Configuration**	"Using Disk Management and configuring RAID 1" on page 23-38
	Date and Time	"Setting the system date and time" in Chapter 6 in the *Wave Server Installation Guide*
	User/Group Management	"Using the User/Group Management applet" on page 2-15
	Local TAPI Configuration	
	Microsoft RRAS	Chapter 21
	Network Connections	Chapter 21
Diagnostics	**System Information**	Microsoft System Information Help
	Performance Monitor	Microsoft Management Console Performance Help
	Task Manager	Microsoft Windows Task Manager Help
	Event Viewer	Viewing the Wave Event Log
	Network Monitor	Microsoft Network Monitor Help

Starting a remote access applet

When you start a remote access applet from the Management Console, Wave ISM attempts to start a Remote Desktop Connection:



Do you trust the computer you are connecting to?

Before connecting to the following remote computer, verify that you trust the computer to have access to your credentials and connected devices.

Name of the remote computer:
192.168.168.12

Credentials
Password for econnect

Connected devices
Changes to these options apply for this connection only.

☑ Allow access to your local clipboard

Important: Verify that the settings being used for this connection are coming from a trusted source.

Do you wish to continue and connect to this computer?

Click **Yes** to continue. For the User/Group Management applet only, you are presented with the Vertical Wave Global Administrator Log On dialog, with your logon credentials already filled in. Click **OK** to continue. See “Using the User/Group Management applet” on page 2-15 for more information.

Exiting a remote access applet

When you are done using the application, choose **Exit** from your browser's File menu, or click the **X** at the upper right of the application window to return to the Management Console.

Click

Important! You can click the System Desktop icon at the top of the Management Console in order to access other resources on the Wave Server (as opposed to running another Management Console applet.) To then return to the Management Console, you **must** log off from the Windows Desktop. If you do not log off, you will keep that remote session open, possibly locking out other administrators from being able to use Remote Desktop to access the same or another remote access applet, since only a limited number of remote sessions may be configured on your system.

To log off from the Windows Desktop, choose **Start > Logoff**.

If you are having trouble establishing the Remote Desktop Connection...

If you have trouble establishing a Remote Desktop Connection, check your browser proxy settings.

To check the proxy settings

1. From the Tools menu of Internet Explorer, choose **Internet Options**.
2. Click the Security tab.
3. If necessary, click the Local intranet icon to select it.
4. Click the **Sites** button.
5. If necessary, select the **Include all sites that bypass the proxy server** option.
6. Click the **Advanced** button.
7. Enter the specific Wave host name in the **Add this Web site to the zone** field.
8. Click **Add**.
9. Click **OK** to save your changes until all dialogs are closed.

Left-handed mouse users

Once a Remote Desktop Connection is established, a user with a left-handed mouse may notice that the mouse buttons suddenly appear to become unresponsive. In actuality, the mouse buttons have been reassigned to right-handed settings, and the buttons are now reversed. This happens because when you connect to a PC via a Remote Desktop Connection, mouse and keyboard settings are inherited from the PC to which you connect.

Navigating applet tree structures

Several of the Management Console applets employ tree structures to represent the items you are configuring. For example, the Trunk Configuration applet uses a tree structure to represent cards or modules and the trunks and channels you are configuring.

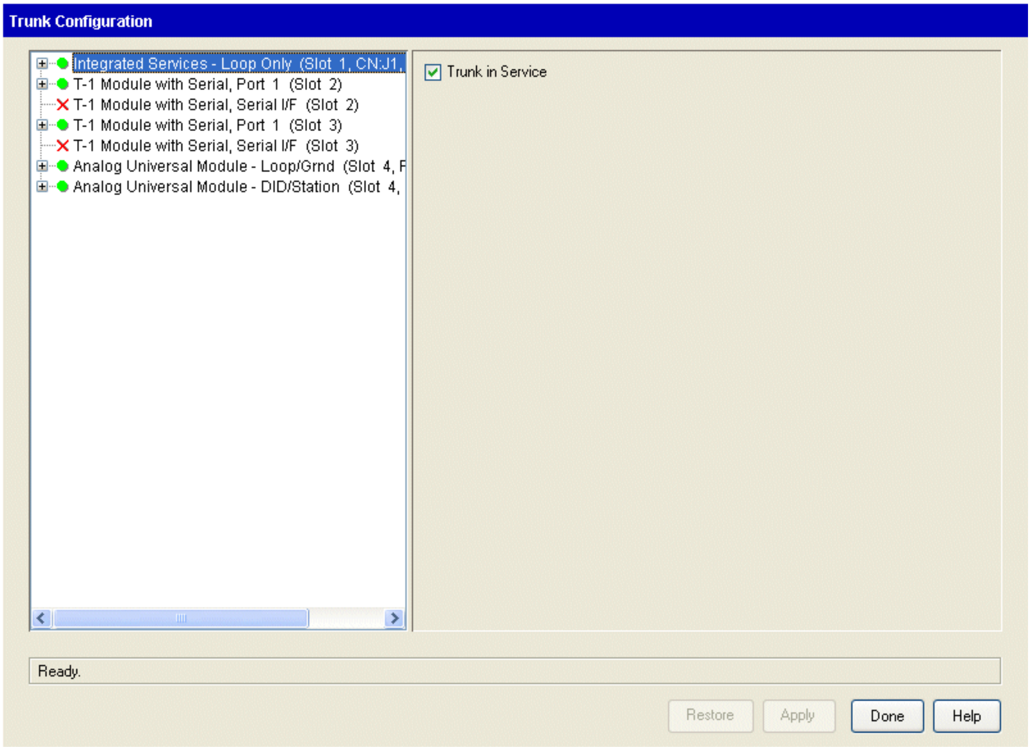
Navigating applet tree structures typically includes the following:

- Displaying and hiding items in a tree (for example, the channels of a card or module in the Trunk Configuration applet)
- Selecting items in a tree

Displaying and hiding items in a tree

To display items in a tree

1 Open the appropriate applet, if it is not already open.


Trunk Configuration

- ● Integrated Services - Loop Only (Slot 1, CN:J1,
- ● T-1 Module with Serial, Port 1 (Slot 2)
- ✕ T-1 Module with Serial, Serial I/F (Slot 2)
- ● T-1 Module with Serial, Port 1 (Slot 3)
- ✕ T-1 Module with Serial, Serial I/F (Slot 3)
- ● Analog Universal Module - Loop/Grnd (Slot 4, F
- ● Analog Universal Module - DID/Station (Slot 4,

☑ Trunk in Service

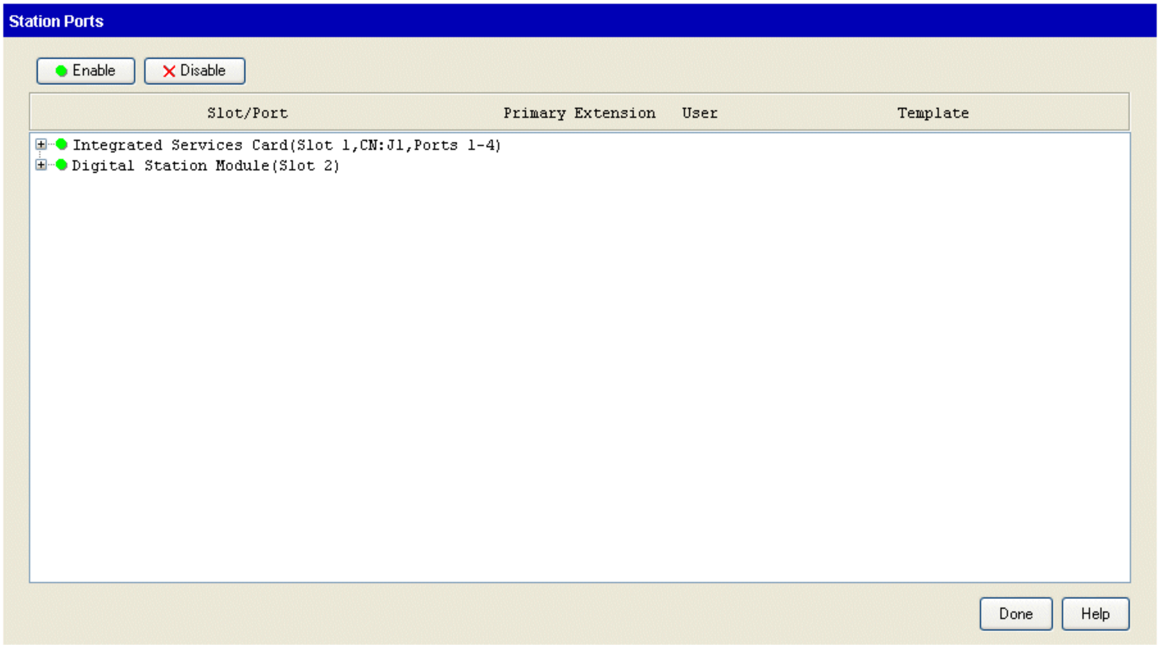
Ready.

Note: A green dot next to a trunk, channel, port, or card, or module indicates that it is in service. A red X indicates that the item is not in service.

2 Click the plus (**+**) sign next to the appropriate module or card to display the items within it.

To hide items in a tree

1 Complete any configuration changes you are making in dialogs opened from an applet, and return to that applet. The Station Ports applet is shown in the following example.



Station Ports

● Enable ✕ Disable

Slot/Port	Primary Extension	User	Template
⊞ ● Integrated Services Card(Slot 1,CN:J1,Ports 1-4)			
⊞ ● Digital Station Module(Slot 2)			

Done Help

2 Click the minus (-) sign next to the appropriate trunk, module, or card to hide the items within it.

Selecting items in a tree

To select items in a tree

1 Open the appropriate applet, if it is not already open, and display the items within a trunk, card, or module.

2 Select the items you want to configure.

- To select a contiguous range of items, select the first item in the range, then hold down the Shift key while you select the last item in the range.
- To select a noncontiguous range of items, hold down the Ctrl key while you select each item.

When you access dialogs containing values that apply to the selected channels, what you see depends on which channels are selected:

- If all channels selected have the same values, those values are displayed
- If all channels selected have the same values, and those values are the default values, the word Default is displayed
- If the channels selected have different values, the expression No Common Value is displayed. In the case of check boxes with different values, the check boxes are deselected and (No Common Value) is appended to their labels

Using the User/Group Management applet

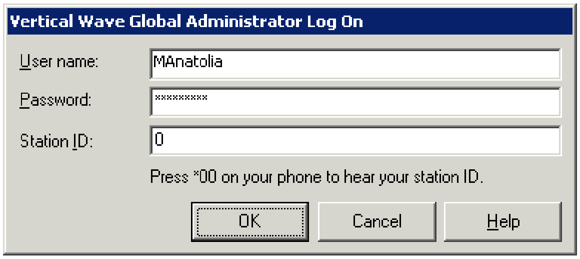
The User/Group Management applet is a remote access applet that lets you configure users as well as access many other Wave configuration and monitoring tools.

Accessing the User/Group Management applet

To access the User/Group Management applet

Click

1. From the Wave Global Administrator Management Console, click the **User/Group Management** icon, located in the PBX Administration section.
2. A remote access session opens, connecting you to the Vertical Wave Global Administrator Log On dialog, with your Wave ISM logon credentials already entered.



Vertical Wave Global Administrator Log On

User name: MAnatolia

Password: *********

Station ID: 0

Press *00 on your phone to hear your station ID.

If your name and password do not appear, enter them.

Note: A username called "Admin" exists by default, with a password of 100. To create other administrators, you must add users and give them Global Administrator permissions (see "The Security \ Permissions tab" on page 11-96).

3. Do one of the following:
   - Enter your phone's **Station ID**. To do so, press *00 on your telephone to retrieve your station ID, and then enter that number. You must enter your station ID if you will need to record an auto attendant prompt or user voice title using the audio controls. (See "Using the audio controls" on page 2-21.)
   - Leave **Station ID** set to 0 if you do not need to use the audio controls. The audio controls will be disabled in the various User/Group Management applet views.
4. Click **OK**. The User/Group Management applet opens.

Note: Leaving the Admin user password as 100 is a security risk that can cost your company money due to toll fraud. For more information about system security, see Appendix A.

The User/Group Management applet interface

The User/Group Management applet interface is composed of *views* (see “Working in views” on page 2-18). Each view enables you to configure, manage, or monitor an aspect of the Wave system.

Users	Manage Wave users. Includes changing passwords and allocating disk space to users for voicemail messages and greetings.	“The Users view” on page 11-8
Groups	Manage ViewPoint Groups (groups of related extensions or contacts).	“The ViewPoint Groups view” on page 12-4
Pickup Groups	Manage Pickup Groups (groups of extensions that can be answered by all the users in the group).	“Configuring call pickup groups” on page 16-5
Dialing Services	View external first digits and configure how they appear in ViewPoint	“Configuring how first digit extensions appear in ViewPoint” on page 9-3
Auto Attendants	Manage auto attendants that handle and route inbound calls with voice menus.	“Creating a new auto attendant” on page 13-3
Queues	Manage groups of agents in Wave Contact Center queues.	*Wave Contact Center Administrator Guide*
Maintenance Log	View a log recording Global Administrator actions.	“Using the Maintenance Log view” on page 22-3

Dial Plan	View and edit a complete list of internally dialable numbers.	"Managing your dial plan with the Dial Plan view" on page 22-2
System Prompts	Listen to and change recordings used for standard system prompts and auto attendants.	"The System Prompts view" on page 18-2
Call Log	View a record of all the calls made on the system.	"Using the Call Log view" on page 22-5

Using the Tools menu

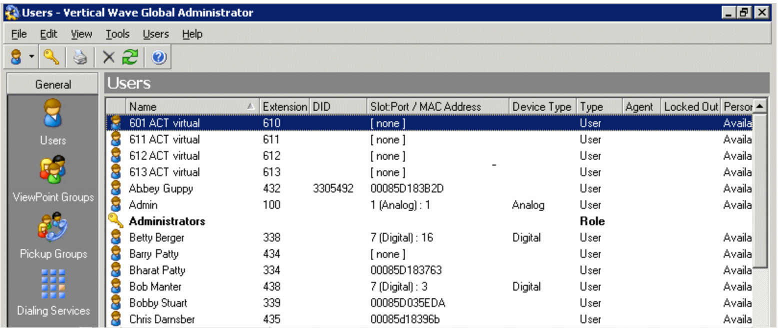
The Tools menu of the User/Group Management applet offers additional Wave features not available from the views:

Update Access Codes	Change the access code used for a particular dialing service.	"Changing an access code in a user's saved numbers" (page 9-39)
Recalculate Disk Usage	Update each user's total disk usage (how much space the user's audio files are taking up), displayed in the Users view and when you edit an individual user.	"Viewing the user's disk usage" on page 11-93
Analyze Security	Analyze your system to identify users whose passwords do not fall within password security settings guidelines, and which may make your system vulnerable.	"Securing your system against toll fraud" on page A-3
User Templates	Open the User Template dialog to create a new user template or edit an existing one.	"Creating and updating users via a user template" on page 11-107

Columns	Customize the columns that appear in each view.	“Customizing columns” (page 2-20)
Options	Customize the appearance of names, Call Log size, and defaults for station and extension numbers.	“Assigning an extension” on page 11-16 “Displaying a specific number of Call Log entries” (page 22-10)
System Settings	Configure and customize several aspects of your Wave system.	Chapter 4

Working in views

To open a view, click its button in the view bar on the left side of the User/Group Management applet window.



Name	Extension	DID	Slot:Port / MAC Address	Device Type	Type	Agent	Locked Out	Persor
601 ACT virtual	610		[none]		User			Availa
611 ACT virtual	611		[none]		User			Availa
612 ACT virtual	612		[none]		User			Availa
613 ACT virtual	613		[none]		User			Availa
Abbey Guppy	432	3305492	00085D183B2D		User			Availa
Admin	100		1 (Analog) : 1	Analog	User			Availa
Administrators					**Role**			
Betty Berger	338		7 (Digital) : 16	Digital	User			Availa
Barry Patty	434		[none]		User			Availa
Bharat Patty	334		00085D183763		User			Availa
Bob Manter	438		7 (Digital) : 3	Digital	User			Availa
Bobby Stuart	339		00085D035EDA		User			Availa
Chris Darnsber	435		00085d18396b		User			Availa

You can also open a view by clicking the **View** menu and choosing a view.

Note: If a view is not available to you, you might not have permission to view it. Check with your system administrator, or see “The Security \ Permissions tab” on page 11-96.

The main part of a view contains rows of the *items* that pertain to that view. For example, in the Users view, each Wave user is displayed as an item on a row. Double-click an item to edit it.

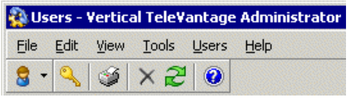
Using commands in a view

A command always affects the item or items that are selected. To select multiple items, hold down the CRTL key as you click the items. You can perform a command using any of the following methods:

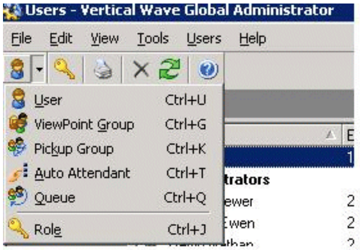
- Choose a command from the view’s menu. For example, in the Users view, click the **Users** menu and choose a command.
- Click a toolbar button (see the next table).
- Right-click an item and choose a command from the shortcut menu that opens. This is often the fastest way to perform a command.

Using the User/Group Management applet toolbar

The User/Group Management applet toolbar is located on the main menu bar in each view. It gives you quick access to several User/Group Management applet commands that are also available through the User/Group Management applet menus.


Users - Vertical TeleVantage Administrator
File Edit View Tools Users Help

To create a new item when you are working in any Wave view, click the arrow next to the first button on the toolbar and select an item.



Customizing columns

Click a column header to sort by that column. Click again to sort in the reverse order. The arrow in the column header shows by which column and in what direction the display is currently sorted.

You can resize column widths by dragging the sides of the column headers.

For each view in the User/Group Management applet, you can choose the columns that you want to see and the columns that you want to hide. Some views do not show all the available columns by default.

To show or hide columns in a view

1. Choose **Tools > Columns,** or right-click a column header. The Columns dialog opens.
2. From the **View** drop-down list, choose the view you want to change.
3. Check a column to show it. Uncheck a column to hide it. For an explanation of the various columns, click **Help**.
4. Click **OK**.

Working with voice files

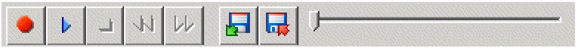
A voice file is an audio recording that is stored as a file. Wave stores system prompts, greetings, voice messages, and recorded conversations in voice files that you can play over your computer speakers or on the phone. You can record voice files using the phone.

Wave voice files are in WAV format, but you can import files of other formats.

Note: When archiving voice messages or call recordings you can specify MP3 as the file format. See “Archiving call recordings and voicemail” on page 22-24.

Using the audio controls

Wave's audio controls make it easy to create and modify recordings of all types. The following controls appear in Wave wherever you can create and listen to recordings.



To create and play recordings, use the buttons on the audio controls as shown in the following table and speak into your phone.

Record ●	When you are ready to record, pick up your phone, and then click **Record**. A beep signals that recording has begun.
Play ▷	Click **Play** to listen to the recording.
Stop □	When you are done recording, click **Stop** first and then hang up. If you simply hang up, you will introduce an audible click at the end of the recording.
Fast Forward ▷▷	Click **Fast Forward** to skip ahead while listening to the recording.
Rewind ◁◁	Click **Rewind** to skip back while listening to the recording.

To move forward and backward within the recording, drag the slider bar.

Importing and exporting voice files

To import or export a voice file, use the import or export buttons on the recording control, as shown in the following table.

Import	You can import a voice file in WAV format to use for any Wave recording (greetings, voice titles, and so on). Wave can import WAV files with a frequency of 8Khz, 11.025 Khz, 22.05 Khz, or 44.1 Khz.
Export	You can export any of your recordings, including system prompts and voice titles, to a WAV file or an MP3 file.

Chapter 3

Before You Begin

CHAPTER CONTENTS

Before you begin

Before you configure your Wave system, make sure the following installations and records are complete:

- Cabling and hardware installations
- Trunk (or service) confirmation letter from your phone service provider
- Your Configuration and Design Worksheets (from your Vertical Communications reseller) on trunking, extensions, incoming and outgoing call flow, voice mail access, and your dialing plan

To manage your Wave system, you need a client workstation with the following minimum configuration:

- A PC running Microsoft Windows 2000, Windows XP, or Windows Server 2003 and at least 256MB of RAM
- LAN or WAN connectivity through an Ethernet card or modem

- Microsoft Internet Explorer 6.0 Service Pack 1

Important! Some of the Management Console applets display dialogs, warnings, and panels automatically. If you have installed a browser pop-up blocker on your client PC, these pop-ups may not appear. You can usually configure blocker software to allow pop-ups from specific domains or IP addresses.

About the General Settings applet

You use the General Settings applet to set many system-wide settings for your Wave system. The following list provides links to information about the tasks you can accomplish via the various tabs in the General Settings applet.

System tab

- **Company Name, Main Number, Serial Number, Voice Mail System**. See “Entering basic system information” on page 3-4.

  Note: During system installation, you will already have used the General Settings applet to enter some basic system information, as described in Chapter 6 in the *Wave Server Installation Guide*.

- **Locale**. See “Setting and viewing system locale settings” on page 33-1.
- **Notify when less than ___ megabytes free**. See “Setting the minimum free hard drive space notification limit” on page 23-24.
- **Enable IMpulse Instant Message Service**. See “Enabling the Instant Messaging server” on page 16-44.
- **ViewPoint Mobile Port**. See “Changing the ViewPoint Mobile Port” on page 11-6.

PBX tab

- **Enable Public Address**. See “Enabling Public Address” on page 16-26.
- **Allow Automatic Phone Relocation**. See “Enabling automatic phone relocation” on page 16-26.
- **Enable DSS/BLF updates when the user’s phone is active on any line**. See “Enabling DSS/BLF updates when the user’s phone is active on any line” on page 16-29.
- **Music On Hold**. See “Configuring Music On Hold” on page 16-21.
- **External Caller ID**. See “Configuring system-wide Caller ID settings” on page 16-11.

- **Night Answer Service**. See “Configuring Night Answer” on page 16-31.
- **Fax Redirect Service**. See “Configuring Fax Redirect” on page 16-15.

PBX (Advanced) tab

- **Use Forwarding Target of Last Destination in Chain**. See “Configuring calls to be forwarded to the RNA forwarding target” on page 13-26.
- **Suppress ring if receiving page**. See “Suppressing ringing on any digital phone that is receiving a page” on page 3-11.
- **Stutter Dial Tone Duration (Seconds)**. See “Setting the message-waiting dial tone duration” on page 3-11.
- **Call Park**. See “Configuring Call Park options” on page 16-4.
- **Trunking**. See “Configuring external call routing restrictions” on page 16-14.
- **When dialing, wait up to ___ seconds for next digit to be entered**. See “Configuring dialing time-out” on page 16-13.
- **Require external access code to dial emergency numbers**. See “Requiring an access code for emergency number dialing” on page 16-13.
- **Enable Call Return ___ Trunk Access Code (TAC)**. See “Enabling call return for external calls” on page 16-30.

WaveMail tab

- See “Synchronizing a user’s Wave voice messages and contacts with the user’s e-mail program” on page 11-30.

ISDN tab

- **Outbound Caller ID, Inbound Caller ID**. See “Configuring system-wide ISDN settings” on page 17-12.

Fault Monitor tab

- **View Fault Monitor Error Logs**. See “Viewing the Fault Monitor Error Logs” on page 23-19.

Time Service tab

- See “Configuring the time service” on page 3-12.

Entering basic system information

Note the following about the information you enter according to the following instructions:

- **Company Name** and **Main Number** are both used in your external Caller ID.
- The Wave Server **Serial Number** is used by Global Manager to identify each Wave Server uniquely. Also, your Vertical Technical Support representative may request it while troubleshooting a problem.
- The **Locale** that you specify enables appropriate locale-specific system settings including ring cadence, minimum analog hook flash, tone set, line impedance, trunk locale, and so forth. For more about changing the **Locale** setting, see “System Locale Settings” on page 33-1.
- **Voice Mail System** specifies the extension that users dial, or trunks group use, to reach the voice mail hunt group. The default VoiceMail extension is 550. If you want to use a different extension to access voicemail, see “Configuring the VoiceMail extension” on page 7-7.

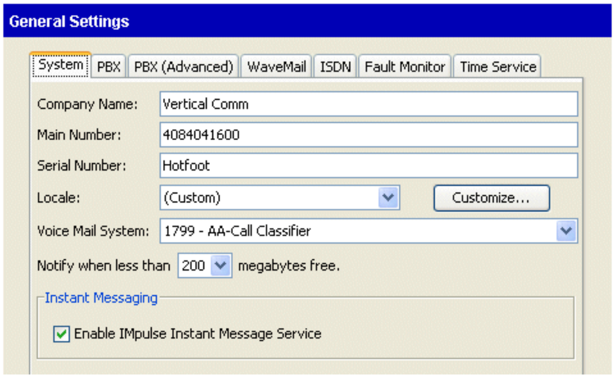
To enter the basic system information

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Click the System tab.


General Settings

Company Name: Vertical Comm
Main Number: 4084041600
Serial Number: Hotfoot
Locale: (Custom)
Voice Mail System: 1799 - AA-Call Classifier
Notify when less than 200 megabytes free.
Instant Messaging
☑ Enable IMpulse Instant Message Service

4 Enter your **Company Name**.

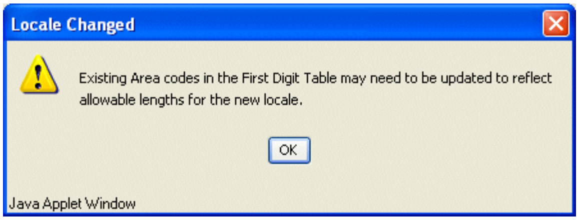
5 Enter your company’s **Main Number**, for example 6173540600. You cannot enter parentheses, spaces or dashes.

6 Enter the entire **Serial Number** of the Wave Server. The serial number is located on the side of the chassis, and is in the following format, where AA is an alphabetical value and n is a numerical value:

AAnnnnnnnnnn

7 If the **Locale** setting is correct for your system, go to step 8. If not, select your locale from the drop-down list.

When you change the **Locale** setting, you are reminded that you may need to update any area codes that you have already defined in the First Digit Table to reflect new area code requirements for the selected locale.



Locale Changed

Existing Area codes in the First Digit Table may need to be updated to reflect allowable lengths for the new locale.

For more about editing the First Digit Table, see “Setting the home area code” on page 7-5.

Caution! *The Customize button allows you to customize the advanced settings for the locale specified. The default advanced settings for a locale should work for you unless you have a unique environment. These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative. For more about the advanced settings for a locale, see “System Locale Settings” on page 33-1.*

Click **OK** to continue.

8 Select the **Voice Mail System** extension used to reach the voice mail hunt group. The default is 550 (which is adequate for most systems) but you can map it to a different pilot number (see “Configuring the VoiceMail extension” on page 7-7.)

9 Click **Apply** to save your changes.

10 Click **Done** to return to the Management Console.

Verifying installed components

You can verify that all of your installed cards and modules are recognized by the Wave system and functioning properly by using the Chassis View applet. Chassis View shows all cards and modules installed in the Wave chassis; LEDs display status dynamically.

To verify installed components

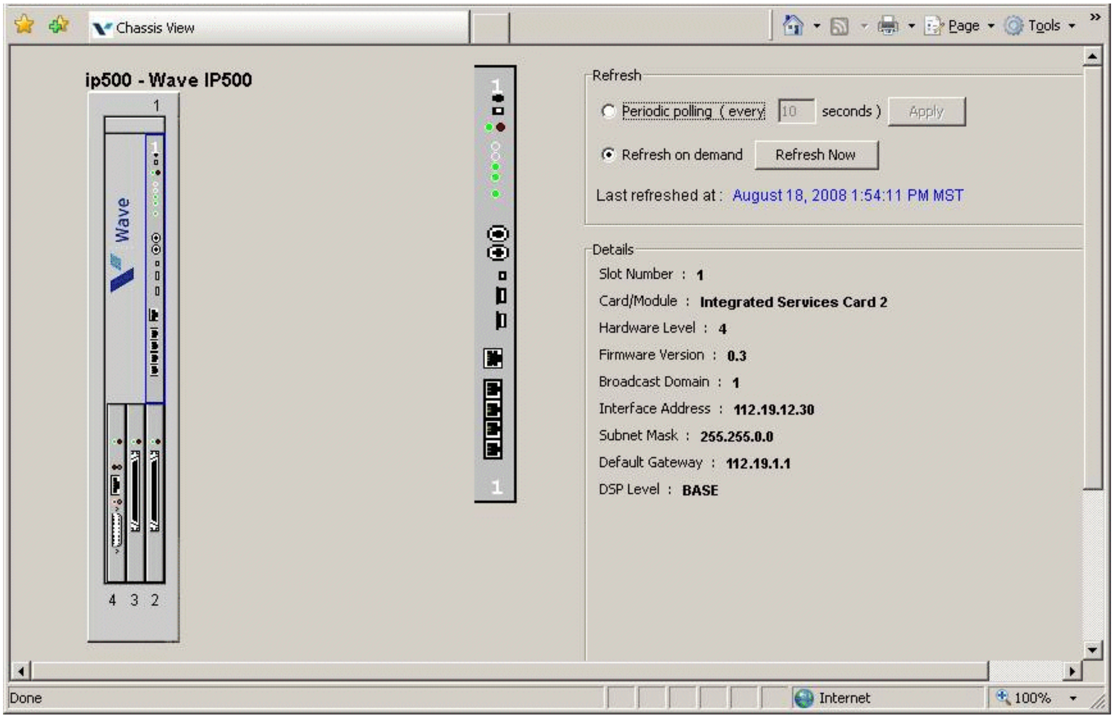
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Chassis View icon, located in the General Administration section.

3 Make sure all the cards and modules you have installed are visible in the graphical representation of your Wave chassis. The Chassis View looks different depending on your Wave Server model.

On the Wave IP 500 Server, the Chassis View looks like this:



Refresh

○ Periodic polling (every 10 seconds) Apply

● Refresh on demand Refresh Now

Last refreshed at : August 18, 2008 1:54:11 PM MST

Details

Slot Number : 1

Card/Module : Integrated Services Card 2

Hardware Level : 4

Firmware Version : 0.3

Broadcast Domain : 1

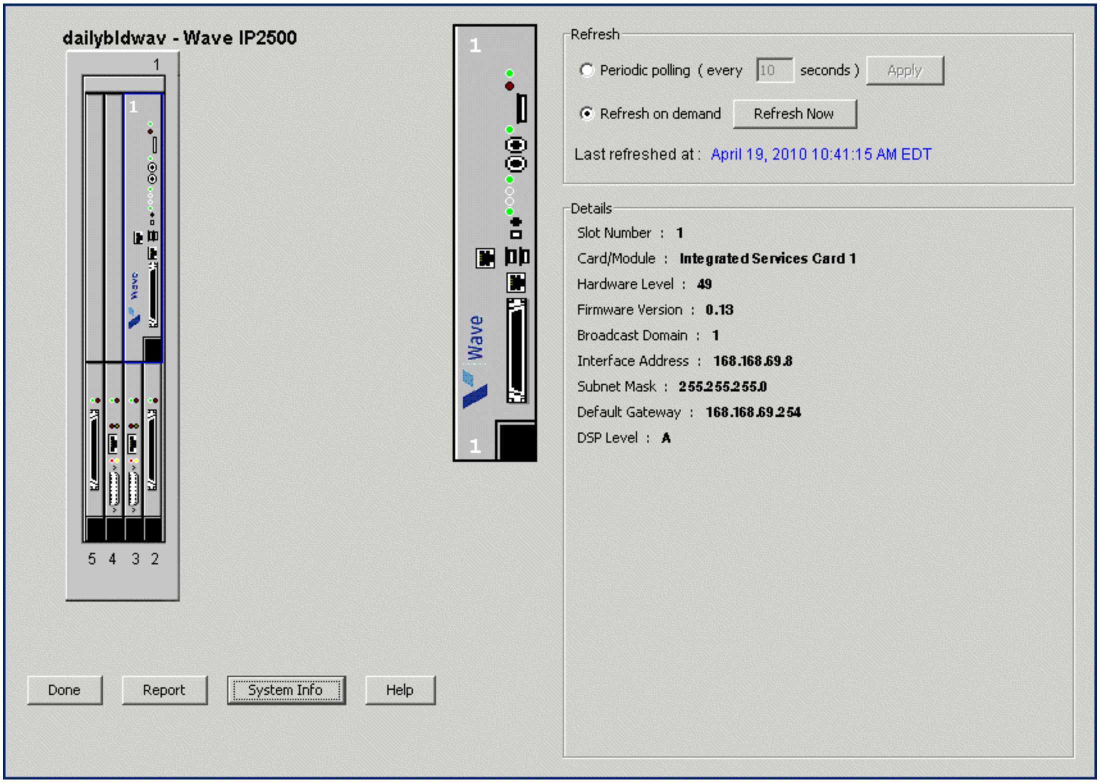
Interface Address : 112.19.12.30

Subnet Mask : 255.255.0.0

Default Gateway : 112.19.1.1

DSP Level : BASE

On the Wave IP 2500 Server, the Chassis View looks like this:



dailybldwav - Wave IP2500

Refresh

○ Periodic polling (every 10 seconds)

● Refresh on demand

Last refreshed at : April 19, 2010 10:41:15 AM EDT

Details

Slot Number : **1**
Card/Module : **Integrated Services Card 1**
Hardware Level : **49**
Firmware Version : **0.13**
Broadcast Domain : **1**
Interface Address : **168.168.69.8**
Subnet Mask : **255.255.255.0**
Default Gateway : **168.168.69.254**
DSP Level : **A**

Position the cursor on a card or module to display an expanded version of it, along with statistics for that card or module, to the right of the representation of the entire chassis. Clicking a card or module takes you to the appropriate configuration applet.

4 If a card or module is not visible in Chassis View, check the physical LEDs to make sure they are green (on and operational).

If the physical LEDs are red (nonoperational):

a Shut down and then power off the Wave system.

b Reseat the card or module.

c Restart the system, reopen your browser window, and check Chassis View again.

d Verify that the components that were not visible now show as functioning in Chassis View.

5 Click **Done** to return to the Management Console.

Adding accounts and passwords

To secure your Wave system against unauthorized configuration, you must remove the default account and replace it with a new account.

By default, only individuals with enterprise-level access can configure the Wave system using the Management Console.

The Access Permissions applet contains a list of all the Management Console applets and the access level required to use them. You can use the Access Permissions applet to change the level of access granted to manager- and user-level accounts. For more information about configuring access permissions, see page 3-10.

See also the following topics that may apply to your environment:

- Joining Wave to a Windows domain
- Using Windows Active Directory accounts to administer Wave.

To replace the default Wave accounts

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Password Administration icon, located in the General Administration section. The Password Administration applet opens.

3 Click **New** to open the Add New User dialog.

The first user you create will be an enterprise-level user. Enterprise-level access is the most comprehensive. It allows an administrator to perform all of the Wave administrative functions, including changing and configuring access permissions. You will need at least one account with enterprise-level access to configure everything in your Wave system.

4 Enter a **User Name** for the account.

The user name can be up to 20 characters and can use any combination of alphanumeric characters and exclamation points (!), underscores (_), and dashes (-). However, the first character may not be a numeral.

5 Enter the user's **Full Name**.

The full name can be up to 32 characters and can use any combination of characters, including spaces.

6 Enter a **Password** and confirm it in the appropriate fields.

The password can be from 3 to 14 characters in length, and can use any combination of characters except spaces.

Important! See "Securing your system against toll fraud" on page A-3 for important information about enhancing system security via secure passwords.

7 Choose **Enterprise** from the Access Level drop-down list.

8 Click **OK** to close the dialog.

The information you have specified will appear in the account list in the Password Administration applet.

9 Repeat steps 3 through 8 to create additional accounts. (For accounts with lower access levels, choose **Manager** or **User** instead of **Enterprise** in step 7.)

10 Click **Done** to return to the Management Console.

11 To secure your Wave system, you must log off and log on again with your new enterprise-level user name and password, then return to the Password Administration applet and delete the default accounts.

Caution! *Be sure to keep a record of the new account passwords. Once you remove the default accounts, the only access will be through the new accounts. If you lose your enterprise-level password, you must reinstall and reconfigure your system to gain access.*

Configuring access permissions

Access permissions for most of the Management Configuration applets can be customized. One of three access levels—enterprise, manager, and user—can be selected for each applet. When a logged-on user does not have permission to use an applet, its icon appears dimmed to indicate that the applet is unavailable.

Note: The Access Permissions and Password Administration applets are fixed at the enterprise level and cannot be modified.

To configure access permissions

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Access Permissions icon, located in the General Administration section. The Access Permissions applet opens.

3 Scroll through the list to find the applet that you want to modify. (Applets are arranged alphabetically by name.)

The Access Permissions and Password Administration applets do not appear in this list, because they cannot be modified.

4 Select a permission level from the Access Permissions drop-down list for each applet you want to modify.

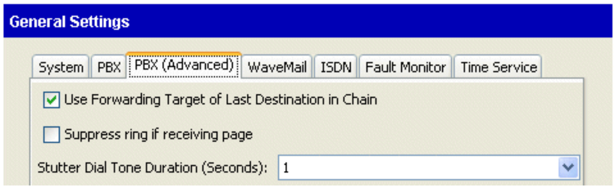
5 Click **Apply** to save your changes.

6 Click **Done** to return to the Management Console.

Setting the message-waiting dial tone duration

The stutter dial tone indicates that a Voice Mail message is waiting on phones that do not have a message-waiting lamp.

In the General Settings applet, PBX (Advanced) tab, you can specify the duration of the dial tone stutter in the **Stutter Dial Tone Duration (Seconds)** drop-down list.



☑ Use Forwarding Target of Last Destination in Chain

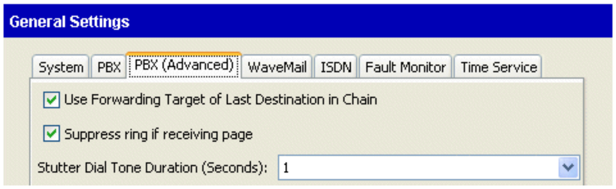
□ Suppress ring if receiving page

Stutter Dial Tone Duration (Seconds): 1

Suppressing ringing on any digital phone that is receiving a page

You can suppress the ringer on any digital phone if a page is being played on that phone. This is a system-wide option that applies to all phones.

To do so, in the General Settings applet, click the PBX (Advanced) tab and then select the **Suppress ring if receiving page** checkbox.



☑ Use Forwarding Target of Last Destination in Chain

☑ Suppress ring if receiving page

Stutter Dial Tone Duration (Seconds): 1

Configuring the time service

The time service polls a specified time server to keep accurate time on the Wave Server for all Wave components.

Note: SIP phones generally get their time settings from the Wave Server, but may require an entry in their configuration files to handle a time zone offset. See the *Vertical Edge 5000 Installation and Configuration Guide* for information on how to make this entry in the phone's configuration file.

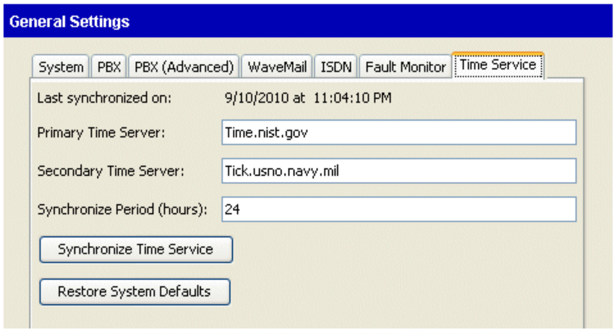
To configure the time service settings

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Click the Time Service tab. The last time the Wave Server was resynchronized is displayed at the top of the tab.



Last synchronized on: 9/10/2010 at 11:04:10 PM

Primary Time Server: Time.nist.gov

Secondary Time Server: Tick.usno.navy.mil

Synchronize Period (hours): 24

4 Enter the domain names of the desired time servers in the **Primary Time Server** and **Secondary Time Server** fields.

Note: You must enter the full name of the time server. Two commonly used time servers are *time.nist.gov* and *tick.usno.navy.mil*.

5 Enter the interval (in hours) between each time server poll in the **Synchronize Period (hours)** field.

6 Click **Synchronize Time Service**. This polls the time server immediately.

7 To verify that the Wave Server was resynchronized, refresh your browser window and click the Time Service tab again. If **Last synchronized on** has been updated, resynchronization was successful.

8 To restore the defaults in each of the Time Service fields, click **Restore System Defaults**.

9 Click **Apply** to save your changes.

10 Click **Done** to return to the Management Console.

Joining the Wave Server to a Windows domain

For security and management reasons, it may be necessary to join the Wave Server to a Windows domain.

Before doing so:

- Verify that the domain policy that will apply to the Wave Server will not force Microsoft Windows Updates to occur on the Wave Server—this can cause the Wave Server to become inoperable.

  Important! All updates for the Wave Server—including Windows Updates—should be applied via Vertical-provided software updates. Vertical works with Microsoft to include all Microsoft updates in regular General Hot Fix packages provided to Wave customers.

- Make sure that the domain policy will not change file permissions or install any additional software on the Wave Server.

For information on Microsoft's Group Policies and how to manage them, see the Microsoft documentation for Windows domains.

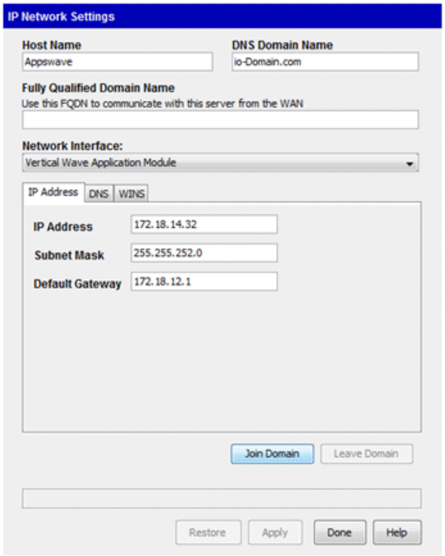
Note: Adding the Wave Server to a Window domain according to the following instructions requires that you restart the Wave Server for the change to take effect.

To join the Wave Server to a Windows domain

1 Before beginning, make sure that the Wave Server is connected to the same network as the domain controller and can ping the domain controller. The DNS server for the Wave Server should already be a domain DNS server.

2 In the Global Administrator Management Console, click IP Network Settings, located in the Data Administration section.

3 In IP Network Settings, click **Join Domain**.



Host Name: Appswave

DNS Domain Name: io-Domain.com

Fully Qualified Domain Name

Use this FQDN to communicate with this server from the WAN

Network Interface: Vertical Wave Application Module

IP Address: 172.18.14.32

Subnet Mask: 255.255.252.0

Default Gateway: 172.18.12.1

4 Enter the domain name and credentials for a valid domain administrator account, and then click **OK**. The Wave Server will be joined to the domain if:

- The Wave Server can communicate with the domain controller.
- The credentials you entered are valid.
- The account you are using has permission to join systems to the domain.

5 Restart the Wave Serverto complete this process.

Note: Once joined to the domain, you still need to use local credentials to log in to the Wave Server. To use domain accounts to log in to the Wave see “Using Windows Active Directory accounts to administer Wave” on page 3-14.

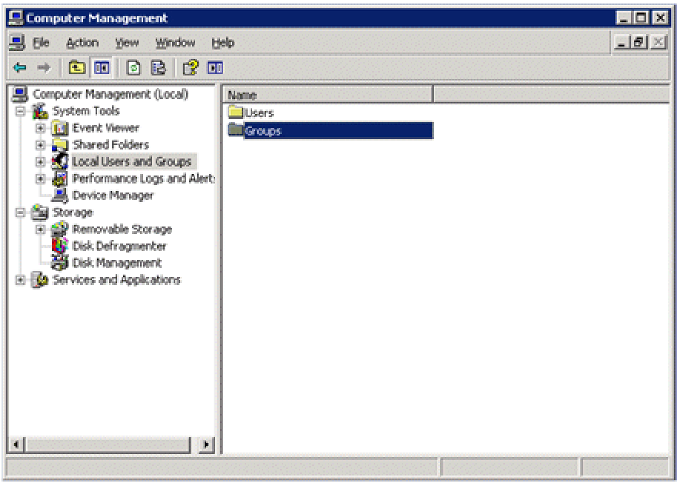
Using Windows Active Directory accounts to administer Wave

If your Wave Server is joined to a Windows domain according to the steps in the previous section, you can use Active Directory accounts to administer Wave.

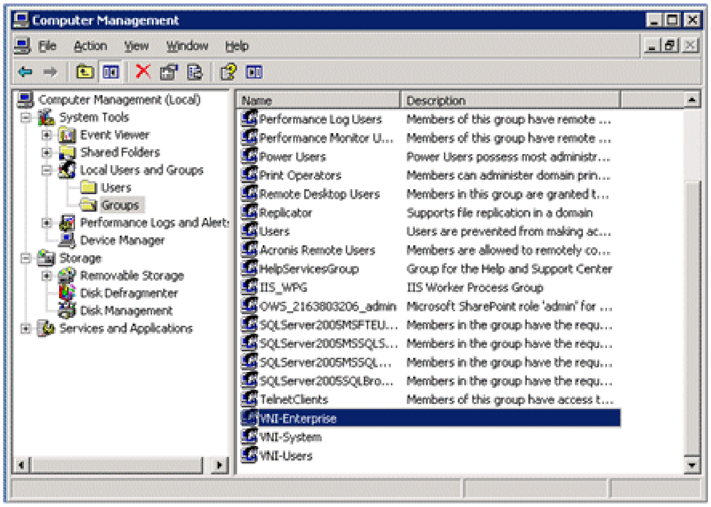
1 Ask your domain administrator to create a domain security group on the domain controller. (See the Microsoft documentation for Windows domains for detailed steps on how to do this.)

2 To enable this security group to administer Wave, on the local desktop on the Wave Server, click **Start > All Programs > Administrator Tools > Computer Management**.

3 In Computer Management, click **Local Users and Group**s, and then double-click **Groups**.

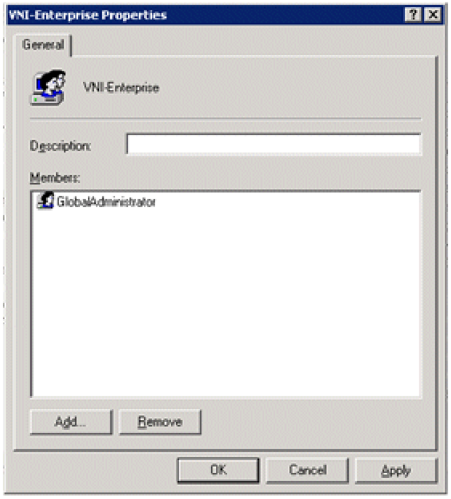


4 Scroll to the bottom of the list of groups and double-click **VNI-Enterprise**.



Name	Description
Performance Log Users	Members of this group have remote ...
Performance Monitor U...	Members of this group have remote ...
Power Users	Power Users possess most administr...
Print Operators	Members can administer domain prin...
Remote Desktop Users	Members in this group are granted t...
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac...
Acronis Remote Users	Members are allowed to remotely co...
HelpServicesGroup	Group for the Help and Support Center
IIS_WPG	IIS Worker Process Group
OWS_2163803206_admin	Microsoft SharePoint role 'admin' for ...
SQLServer2005MSFTEU...	Members in the group have the requ...
SQLServer2005MSSQLS...	Members in the group have the requ...
SQLServer2005MSSQL...	Members in the group have the requ...
SQLServer2005SQLBro...	Members in the group have the requ...
TelnetClients	Members of this group have access t...
VNI-Enterprise	
VNI-System	
VNI-Users	

5 Click **Add** to add your domain security group to this local VNI-Enterprise group.



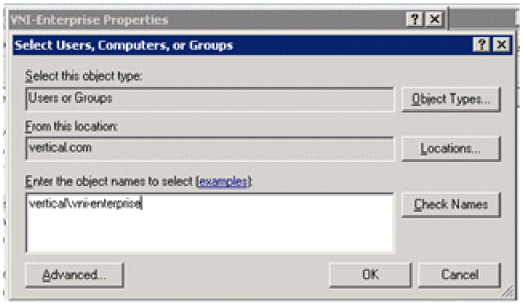
VNI-Enterprise

Description:

Members:

GlobalAdministrator

6 Type in the exact name—including the domain name—of your domain security group and then click **OK**.



VNI-Enterprise Properties

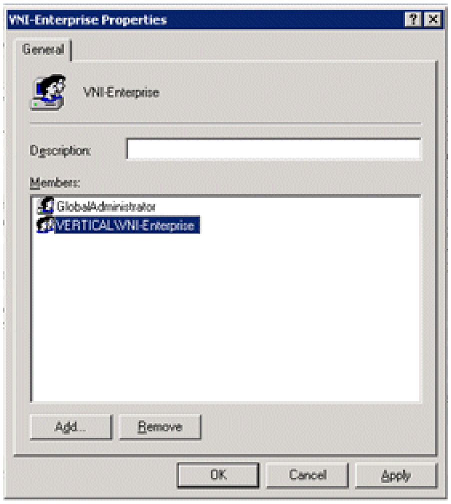
Select Users, Computers, or Groups

Select this object type:
Users or Groups

From this location:
vertical.com

Enter the object names to select (examples):
vertical\vni-enterprise

7 Verify that your domain security group now shows up in the list of members:



VNI-Enterprise Properties

VNI-Enterprise

Description:

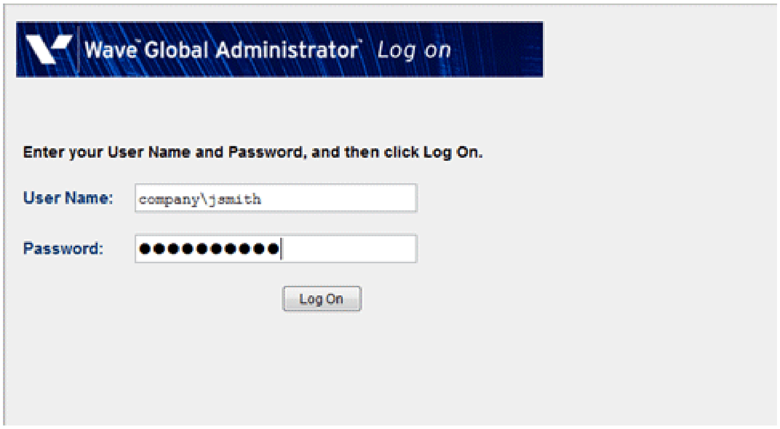
Members:
GlobalAdministrator
VERTICAL\VNI-Enterprise

8 Click **OK**, and then exit Computer Management.

Logging on to Wave using domain credentials

Any users who are listed in or added to your domain security group will now be able to log on to the Global Administrator Management Console using their domain credentials and administer Wave. Their specific credentials are handled in Active Directory.

For example, John Smith has a domain account of jsmith on the domain Company.local. He can log in to Global Administrator Management Console using Company\jsmith as his user name and his domain password:



Enter your User Name and Password, and then click Log On.

User Name: company\jsmith

Password: ●●●●●●●●●●

Note: Active Directory integration applies only to Wave administrators --- it does not extend to ViewPoint usage or voicemail login for regular users.

Chapter 4

System Settings in the User/Group Management applet

CHAPTER CONTENTS

The system settings available through the User/Group Management applet control overall Wave behavior. Before adding Wave users, you should define your system settings.

Opening the System Settings dialog

To access system settings in the User/Group Management applet

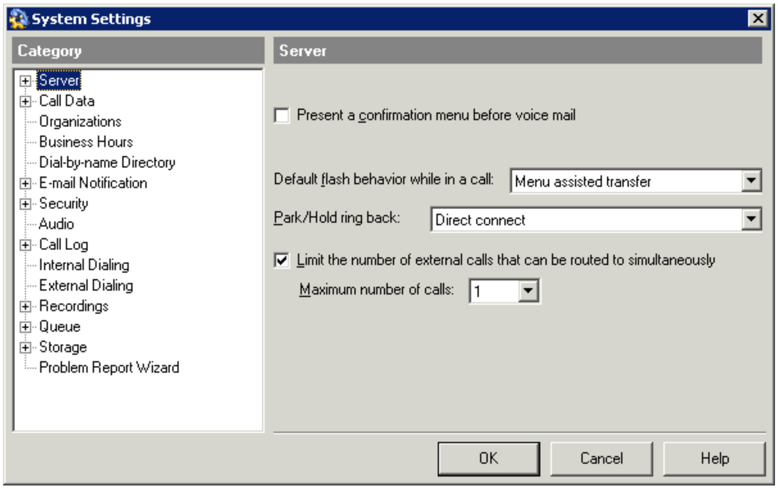
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

The User/Group Management applet opens. See “Navigating applet tree structures” on page 2-11 for information about navigating in the User/Group Management applet.

3 Choose **Tools > System Settings**. The System Settings dialog opens.



Server

□ Present a confirmation menu before voice mail

Default flash behavior while in a call: Menu assisted transfer

Park/Hold ring back: Direct connect

☑ Limit the number of external calls that can be routed to simultaneously

Maximum number of calls: 1

Documentation for the System Settings dialog

The following table shows where to find detailed information for the various tabs of the System Settings dialog:

For information on this tab...	See...
Server	“Setting general Wave settings” on page 4-4
Server \ Network Capture	“Capturing network troubleshooting logs” on page 22-55
Call Data \ Account Codes	“Using account codes” on page 20-10
Call Data \ Custom Data	“Defining a custom data variable” on page 20-19
Organizations	“Using Organizations” on page 20-2
Business Hours	“Setting business hours” on page 4-9
Dial-by-name Directory	“Configuring the dial-by-name directory” on page 4-6
E-mail Notification	“Enabling e-mail notification” on page 4-12
E-mail Notification \ Event Log	“Setting up Wave Event Log notifications” on page 22-16
Security	“Enforcing strong password security” on page 4-14

For information on this tab...	See...
Security \ Permitted Passwords	“Enforcing strong password security” on page 4-14
Security \ Workstation Firewall	Appendix E in the *Wave Server Installation Guide*
Audio	“Setting up system-wide audio options” on page 4-18
Call Log	“Setting Call Log options” on page 22-9
Call Log \ Archive	“Archiving the Call Log” on page 22-11
Internal Dialing	“Changing the internal dial-by-name extension” on page 4-8
External Dialing	“Setting default access codes for callbacks” on page 9-40
Recordings \ Archive	“Archiving mailbox recordings” on page 22-31
Recordings \ System Call Recording	“Recording all calls” on page 19-8
Recordings \ Reminder Beeps	“Including a reminder beep on queue call recordings” on page 19-10
Queue	“When statistics are refreshed” in Chapter 6 in the *Wave Contact Center Administrator Guide*
Queue \ Agent Skills	“Defining skills” in Chapter 3 in the *Wave Contact Center Administrator Guide*
Storage	“Viewing storage statistics” on page 22-40
Storage \ Special Directories	“Changing special Wave directories” on page 22-41
Problem Report Wizard	“Setting Problem Report Wizard defaults” on page 22-45

Setting general options

General Wave options include the following:

- Setting general Wave settings. See the next section.
- Configuring the dial-by-name directory. See page 4-6.

Setting general Wave settings

To set general Wave settings, do the following:

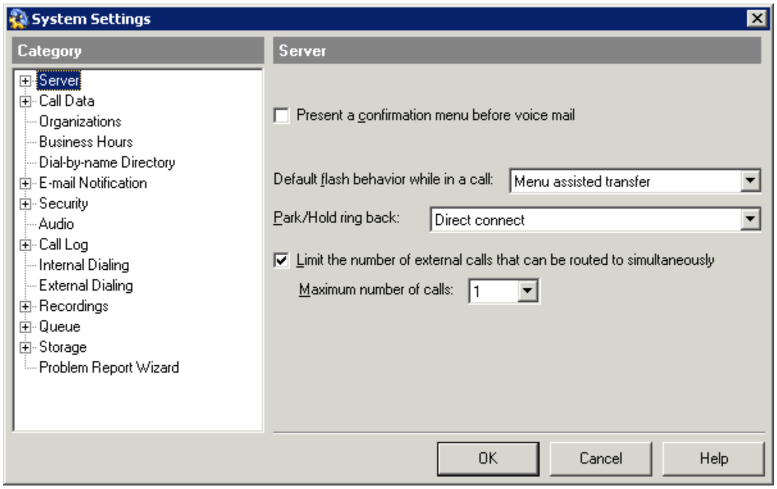
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings.**

4 Click the Server tab.



□ Present a confirmation menu before voice mail

Default flash behavior while in a call: Menu assisted transfer

Park/Hold ring back: Direct connect

☑ Limit the number of external calls that can be routed to simultaneously

Maximum number of calls: 1

5 Define the following settings:

- **Present a confirmation menu before voicemail.** Select this checkbox so that callers hear the confirmation prompt, “To leave a message press 1, or press * to return to the menu” after they hear a user’s voicemail greeting. If not selected (the default), callers go directly to the user’s voicemail after hearing the greeting, where they can record a voice message.
- **Default flash behavior while in a call**. Select the default Flash behavior for analog phones when a user presses **Flash** (or quickly presses the phone’s hook) while on a call. (The default behavior for digital and SIP phones while on a call is to place an active call on hold and return to internal dialtone.)
    - **Menu assisted transfer**. Pressing **Flash** takes the user to the Wave call handling menu, where he or she can put the call on hold, transfer, park, create a conference call, and more. If multiple calls are on hold, the user hears a multi-call menu to select the call to handle.
    - **Direct transfer**. Pressing **Flash** immediately prompts the user for an extension to transfer the call. Use this option to create faster, simplified phone transferring for users who answer and transfer many calls. Note that when **Direct transfer** is selected, a user cannot access the other call handling commands unless he or she has ViewPoint installed.
    - **Manage current call**. Pressing **Flash** takes the user directly to the call handling menu for the current call (the call that was active when **Flash** was pressed.) This option simplifies call handling when multiple calls are on hold. Note that when this option is selected, the user must press **Flash # Flash** to reach the multi-call menu to select a call other than the current call.
- **Park/Hold ring back.** Select what happens when a user answers an automatic ringback call when the ringback interval elapses after leaving a call on hold or parked:
    - **Direct connect**. The user is immediately connected with the caller with no announcing.

- **Limit the number of external calls that can be routed to simultaneously.** When this option is selected, the number of external numbers that can be called simultaneously by a ViewPoint routing list action is limited to the value specified in **Maximum number of calls**, described below.

  Warning! *This checkbox is selected by default—it is HIGHLY RECOMMENDED that you do not change it. If no limit is specified and ViewPoint users create routing list actions that call all members of a ViewPoint Group simultaneously, depending on the number of contacts in the Group all of the trunks on the Wave Server could be tied up making external calls to the contacts.*

  When this option is selected, when a ViewPoint user creates a routing list action that calls all of the members of a ViewPoint Group simultaneously, ViewPoint checks that the Group does not contain more contacts than the number specified in **Maximum number of calls**. If that check fails, the user is informed that “A Group that is called simultaneously cannot have more than *n* contact(s). This setting is determined by your Administrator to conserve phone line usage.”

  Note that a user who is a member of the Group is not counted toward the limit, even if the user’s calls are being forwarded to an external number, because call forwarding is ignored when a user is called as a member of a Group—the call rings the user’s phone, and is not forwarded.

  - **Maximum number of calls**. Maximum number of external numbers that can be called simultaneously by a ViewPoint routing list action. The default value is 1.

6 Click **OK**.

Configuring the dial-by-name directory

The dial-by-name directory enables callers to dial Wave users by name, which is helpful when the extension is not known.

To configure the dial-by-name directory

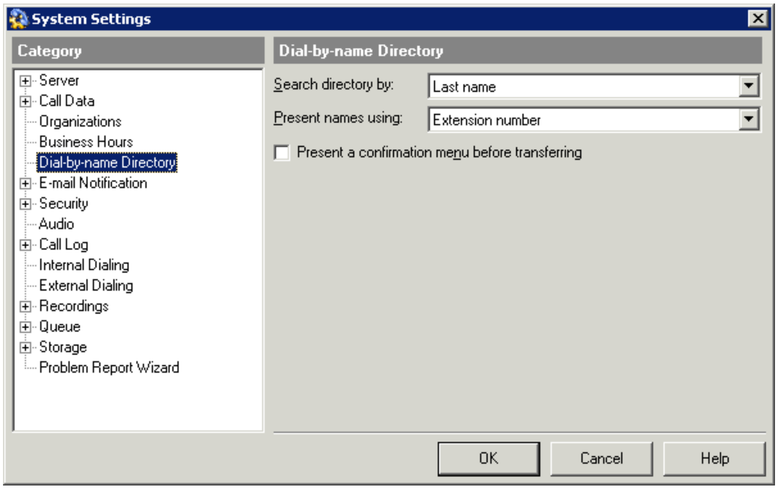
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**.

4 Click the Dial-by-name Directory tab.



Search directory by: Last name

Present names using: Extension number

☐ Present a confirmation menu before transferring

5 In **Search directory by**, select one of the following methods by which a caller can search for a user:

- **Last name**. Caller enters the first few letters of the last name, for example, “sar” for Sargeant. (This is the default method.)
- **First name**. Caller enters the first few letters of the first name, for example, “joh” for John.
- **Last name or First name**. Caller enters the first few letters of either the first or last name.

6 In **Present names using,** select one of the following methods for presenting the names of users to a caller:

- **Extension number**. Caller hears an extension number after each name, for example, “For John Sargent, press 175.” This is the default.
- **Numbered list**. Caller hears a sequence number after each name, as in “For John Sargeant, press 1; for Mary Sargeant, press 2.”

Note: If a voice title is not recorded for a user, the system will read off the extension number in place of the voice title. For example on a match to “John Smith” where John's extension is 201, the system will read "For extension 201 press 201" if there is no voice title recorded for that user.

7 Use the **Present a confirmation menu before transferring** field to specify what happens when a dial-by-name search results in a single match.

- If this checkbox is selected, Wave asks the caller to confirm his or her choice, for example, "For John Sargent, press 1. To try again, press *."
- If not selected, the caller is connected immediately.

8 Click **OK**.

Changing the internal dial-by-name extension

By default, users can dial 411 to access the dial-by-name directory. To change the dial-by-name directory extension, perform the following steps.

Note: When you change the default dial-by-name extension from 411 to another extension, all system prompts that refer to extension 411 automatically update to use the new number. If the new extension requires an alteration to the first digit table, keep in mind that this will cause all of your SIP phones to reboot and download the new dial plan information from Wave when you save your changes.

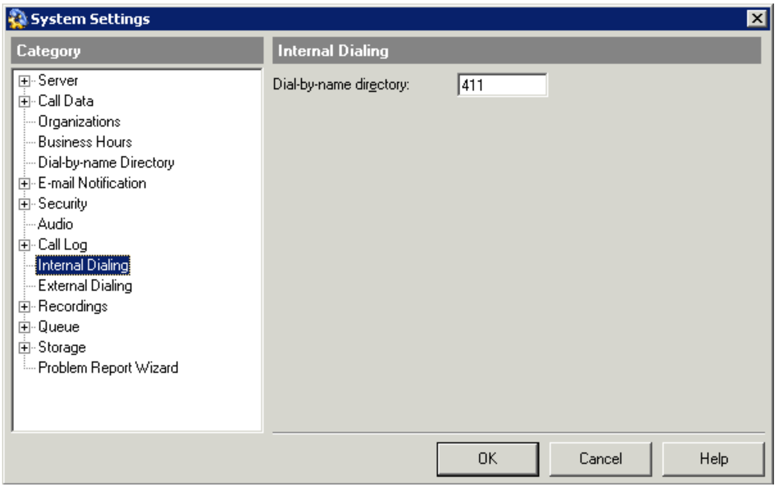
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Click the Internal Dialing tab.



Dial-by-name directory: 411

5 Enter the new extension in **Dial-by-name directory**.

6 Click **OK**.

Setting business hours

Wave uses your business hours settings in schedules that you create for the following:

- **After hours greetings.** See “Scheduling transfers and greetings” on page 13-16.
- **Automatic transfers.** See “Scheduling transfers and greetings” on page 13-16.
- **Notification of new voice messages.** See “Scheduling notifications” on page 11-49.
- **Call rules.** See the *Wave ViewPoint User Guide* for information on how to use call rules.

You can create as many sets of business hours as you need. For example, you can create a set of business hours for the company as a whole (the default), and then create additional sets of business hours for individual Organizations, shifts, and so forth.

Defining business hours

To define your business hours, you define your daily work hours, work days and holidays, as follows:

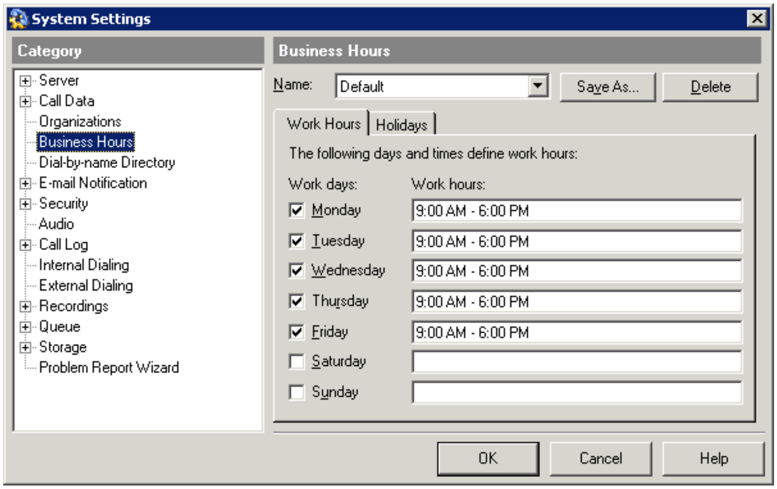
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Click the Business Hours tab.



Name: Default

The following days and times define work hours:

Work days:	Work hours:
☑ Monday	9:00 AM - 6:00 PM
☑ Tuesday	9:00 AM - 6:00 PM
☑ Wednesday	9:00 AM - 6:00 PM
☑ Thursday	9:00 AM - 6:00 PM
☑ Friday	9:00 AM - 6:00 PM
□ Saturday	
□ Sunday	

From the Business Hours tab you can do the following:

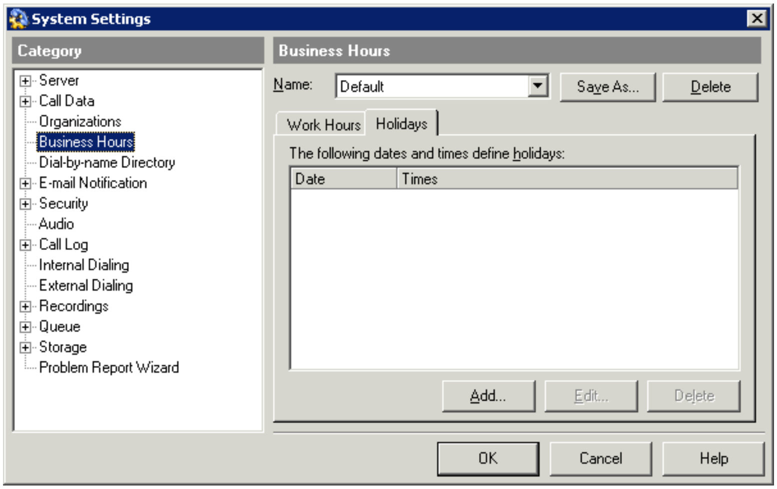
- To create a new set of business hours, fill in the fields as described below, and then click **Save As**.
- To edit an existing set of business hours, select its **Name** from the drop-down list.
- To delete a set of business hours, select its **Name** from the drop-down list, then click **Delete**.

5 On the Work Hours tab, under **Work days**, select a checkbox to count that day as a work day,. Then, under **Work hours**, enter the starting and ending times for each work day.

When you define business hours and holidays, you can type dates and times in most formats. Your entries are converted to a standard format that is based on your Windows regional settings.

Note: You can enter more than one time range for a day, separated by commas, for example, “9:00 AM - 12:00 PM, 3:00 PM - 6:00 PM.” Use this format to express business hour shifts that overlap midnight. For example, to express a shift that runs from 5:00 PM to 2:00 AM the next morning, enter “12:00 AM - 2:00 AM, 5:00 PM - 12:00 AM” for each work day.

6 To define holidays or other special dates, click the Holidays tab.



System Settings

Category: Business Hours

Business Hours

Name: Default

The following dates and times define holidays:

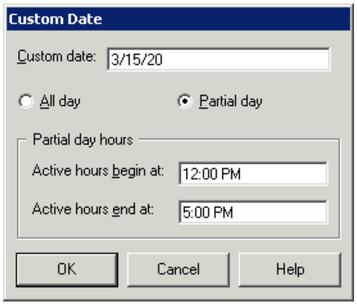
Date	Times

7 Click **Add** to add a new holiday. Click **Edit** to edit an existing one.

8 In the Custom Date dialog, enter the **Custom date** of the holiday.

9 Choose if this is an **All day** or **Partial day** holiday. For a partial day holiday, enter:

- **Active hours begin at.** Starting work time on the holiday.
- **Active hours end at.** Ending work time on the holiday.



Custom Date

Custom date: 3/15/20

○ All day ● Partial day

Partial day hours

Active hours begin at: 12:00 PM

Active hours end at: 5:00 PM

10 Click **OK**.

11 Click **OK** to close the System Settings dialog.

Setting up e-mail notification

Wave can automatically send an e-mail to a user whenever he or she receives a new voice message, and send the voice message audio file as an attachment to the e-mail.

Once you enable e-mail notification for the system, you must configure each user appropriately.

Secure Sockets Layer (SSL) support

SSL provides standard e-mail notifications when you use a hosted service such as Microsoft Office365 or gmail as your company mail server.

When this option is enabled as described below, Wave automatically sends an e-mail to a user whenever he or she receives a new voice message, and attaches the voice message audio file to the e-mail.

Enabling e-mail notification

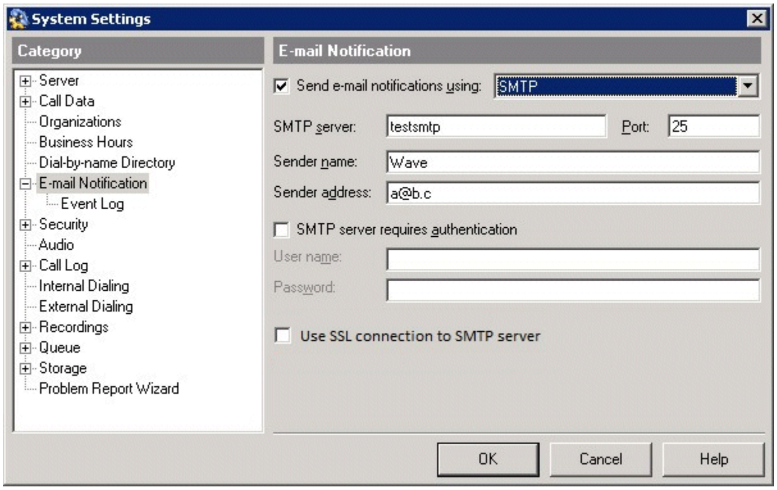
To enable e-mail notification for the system, do the following:

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the User/Group Management icon, located in the PBX Administration section of the Management Console.
3. Choose **Tools > System Settings**, then click the E-mail Notification tab

4 To enable e-mail notification, check **Send e-mail notifications using**. Select **SMTP** from the drop-down list.



E-mail Notification

☑ Send e-mail notifications using: SMTP

SMTP server: testsmtp Port: 25

Sender name: Wave

Sender address: a@b.c

□ SMTP server requires authentication

User name:

Password:

□ Use SSL connection to SMTP server

5 Fill in the following SMTP settings fields with information provided by your e-mail administrator or Internet Service Provider.

- **SMTP server**.
- **Port**.
- **Sender name**.
- **Sender address**.
- **SMTP server requires authentication**. Select this checkbox if valid credentials are required to log on to the SMTP server.
  - **User name**. Username required to log on to the SMTP server.
  - **Password**. Password required to log on to the SMTP server.
- **Use SSL connection to SMTP server**. Select this checkbox if your mail provider requires a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. See “Secure Sockets Layer (SSL) support” on page 4-12.

6 Click **OK**. E-mail notification of voice messages will commence the next time the Wave Server is restarted.

Configuring users for e-mail notification

For information on setting up e-mail notification for a user via the User dialog, see “Setting e-mail notification” on page 11-44.

Enforcing strong password security

Password security is crucial in preventing your company from being victimized by toll fraud. Unauthorized users who gain privileged access to your phone system can place outbound long distance or international calls that get charged to you. In 99.9% of cases, access is gained through insecure (easy-to-guess) passwords. By making your passwords more secure, you can dramatically increase the security of your Wave system against toll fraud. For more information about making your system secure, see Appendix Appendix A.

Recommended minimum password security settings

Important! The following *minimum* password security settings are recommended. Starting with Wave ISM 1.5 SP2, these are the default settings for all *new* installations. On all existing Wave Servers, it is highly recommended that you manually upgrade password security settings to these *minimum* values.

On the Security tab of the System Settings dialog

- Enable the following settings:
  - **Automatically lock out accounts on 3 failed logon attempts**
  - **Automatically clear lockout after 60 minutes**

On the Security \ Permitted Passwords tab of the System Settings dialog

- Set the **Minimum password length** to 5.
- Enable the following settings:
  - **Prevent passwords that contain an account's extension**
  - **Prevent passwords that contain entries from the following list**

    In addition to the passwords listed by default, add any other easily-guessed passwords for example your company name expressed in phone key presses, and so forth.

To enforce strong password security on your system

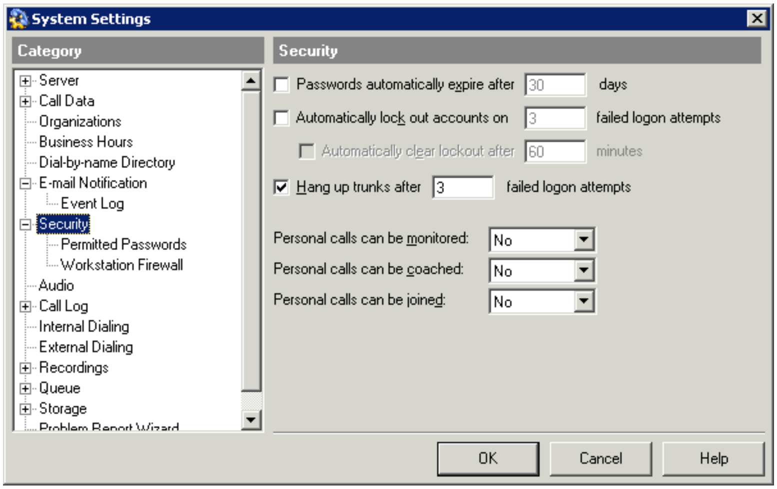
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Click the Security tab.



System Settings

Security

□ Passwords automatically expire after 30 days

□ Automatically lock out accounts on 3 failed logon attempts

□ Automatically clear lockout after 60 minutes

☑ Hang up trunks after 3 failed logon attempts

Personal calls can be monitored: No

Personal calls can be coached: No

Personal calls can be joined: No

5 Use the following options to safeguard your Wave system against unauthorized access:

- **Passwords automatically expire after __ days**. Select this checkbox to force users to regularly change their passwords. Enter the number of days that each user may keep a password before Wave requires them to change it.

  You can override this setting for individual users to permit passwords that never expire. You can also manually force a user to change his or her password whenever you want. See “The Security tab” on page 11-94.

- **Automatically lock out accounts after __ failed logon attempts**. If this checkbox is selected, Wave locks out an account after the number of consecutive failed logon attempts that you specify. A locked-out account cannot log on to Wave, even with the correct username and password, until the Wave administrator unlocks it.

- **Automatically clear lockout after __ minutes**. Select this checkbox to have Wave automatically reopen locked-out accounts after the amount of time (in minutes) that you specify.

  You can also manually reopen a locked-out account in either of the following ways:

  - **User**. In the User dialog / Security tab, click the Other tab, deselect the **User is locked out** checkbox, and then click **OK**.
  - **Queue**. In the Queue dialog / Security tab, click the Account tab, deselect the **Queue is locked out** checkbox, and then click **OK**.

- **Hang up trunks after __ failed logon attempts**. If this checkbox is selected, the system hangs up on any incoming caller who tries to log on to a Wave account with an invalid password after the number of consecutive attempts that you specify.

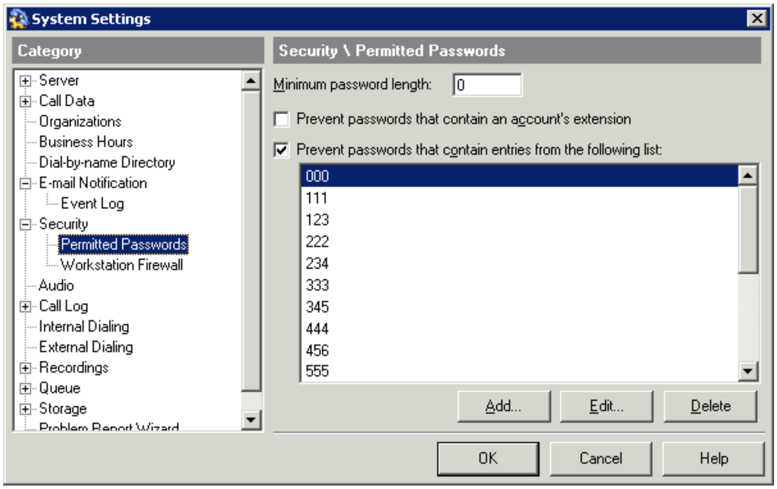
6 Use the following fields to set system defaults for whether a user’s personal calls can be monitored, coached, or joined using the Call Supervising features. Whenever you create a new user, these defaults are used to define if the user’s personal calls can be supervised, and you can override the defaults for an individual user. Set each of the following Call Supervising features to Yes or No.

- **Personal calls can be monitored**. Allows the supervisor to listen in on an active call. Neither the user nor the other parties in the call can hear the supervisor.
- **Personal calls can be coached**. Allows the supervisor to coach a user on an active call. The user can hear the supervisor, but the other parties in the call cannot.
- **Personal calls can be joined**. Allows the supervisor to join another user’s call as a full participant. All parties can hear the supervisor.

Note the following:

- In order for these features to work as expected, the appropriate permissions must be set for the supervisor (**Can coach/monitor/join user calls**) and all users involved in the call (**Personal calls can be coached/monitored/joined**). See “The Security \ Permissions tab” on page 11-96 for more about setting permissions.
- Contact Center queue calls are not personal calls. Monitoring, coaching, and joining queue calls is controlled by Contact Center agent permissions. See the *Wave Contact Center Administrator Guide* for more information.

7 Choose the Security \ Permitted Passwords tab.



Security \ Permitted Passwords

Minimum password length: 0

□ Prevent passwords that contain an account's extension

☑ Prevent passwords that contain entries from the following list:

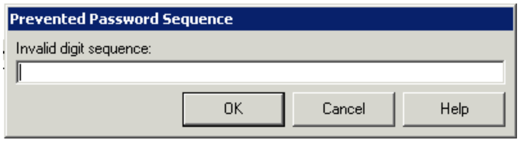
000
111
123
222
234
333
345
444
456
555

Important! By preventing easy-to-guess passwords, you can make your system much more secure from unauthorized access. Vertical highly recommends checking all the options on this tab to prevent toll fraud. When you change any of the options on this tab, users whose passwords are now prohibited will be prompted to change them the next time they log on, and will show up in the Security Analysis report (see Appendix Appendix A)

8 Use the following options to restrict the passwords that users can choose:

- **Minimum password length**. Enter the minimum number of digits for a password. For secure passwords, the minimum should be at least 5, and preferably 7 or more digits.
- **Prevent passwords that contain an account's extension**. A password that contains a user's extension number is especially easy to guess. Select this checkbox to prevent the extension from being any part of the password. For example, a user at extension 337 could not have a password of 337, 33755, or 13378080.

- **Prevent passwords that contain entries from the following list**. Select this checkbox to prevent passwords from containing any of the digit strings in the list. Wave provides a default list of easy-to-guess digit strings, and you can add your own entries to the list.
    - To add a new digit string to the list, click **Add**. To edit the selected digit string, click **Edit**. The Prevented Password Sequence dialog opens:

      Enter the new sequence of digits that users will be prohibited from using as part of their passwords, and then click **OK** to return to the Security \ Permitted Passwords tab.
    - To remove a digit string from the list, select it and click **Delete**.

9 Click **OK**.

For more information about making your system secure, see Appendix Appendix A.

Setting up system-wide audio options

You can set the following audio option on a system-wide basis.

- **Default language used to present system and auto attendant voice prompts to callers and users**. U.S. English is installed by default. French, German, Spanish, and UK English are available in General Hotfix 1005. Note that this HotFix installs system and auto attendant voice prompts, but does not affect the text that appears on a phone’s LED display. To obtain General HotFix 1005, contact your Wave provider.

Note: The **Hold audio file volume** slider control that appears on the Audio tab is not supported in this version.

To change system-wide audio settings

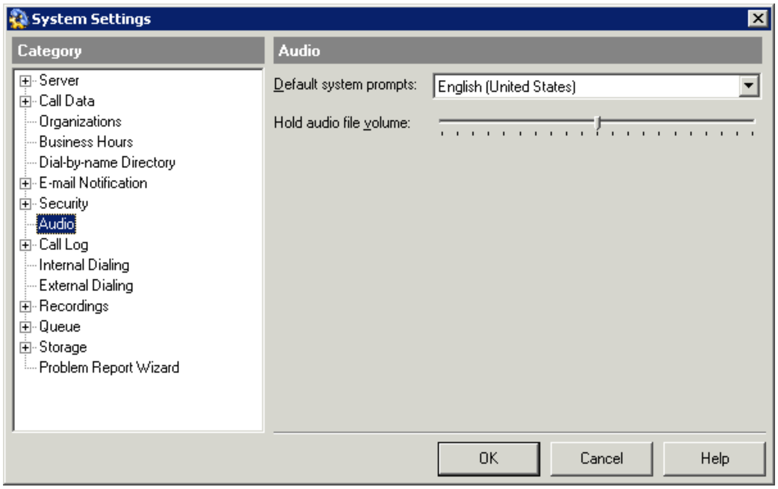
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings.** The System Settings dialog opens.

4 Click the Audio tab.



Default system prompts: English (United States)

Hold audio file volume:

5 Select the language to use to present **Default system prompts** to callers and users from the drop-down list.

6 Click **OK**.

Setting up personal call supervision defaults

You can set system defaults for whether users' personal calls can be Monitored, Coached, or Joined using the Supervise commands. When you create a new user, these defaults are used to define if users' personal calls can be supervised, and you can override the defaults for individual users (see "Configuring whether the user's calls can be supervised" on page 11-95.)

Note the following:

- When you change a system default, users who have that Supervise permission set to "System Default" change to reflect the new default.
- Whether or not a user can *use* the Supervise commands is controlled by permissions. See "Assigning a user's permissions" on page 11-97.

To change personal call supervision defaults

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings.** The System Settings dialog opens.

4 Click the Security tab.

5 In each of the following fields choose **Yes** or **No**:

- **Personal calls can be monitored**. Users with the **Allow monitoring user calls** permission can listen to users' personal (not queue) calls without the monitored user knowing.
- **Personal calls can be coached**. Users with the **Allow coaching user calls** permission can add themselves to users' personal (not queue) calls and be heard by the coached user, but not by the caller.
- **Personal calls can be joined**. Users with the **Allow joining user calls** permission can add themselves to users' personal (not queue) calls as full participants.

6 Click **OK**.

For instructions on supervising calls using the Monitor, Coach, and Join features, see Chapter 6 of the *Wave ViewPoint User Guide*. For information on configuring a user for the permissions needed to Coach, Monitor or Join another user's personal calls, see "Assigning a user's permissions" on page 11-97. For information on supervising queue calls, see the *Wave Contact Center Administrator Guide.*

Chapter 5

Configuring Analog and Digital Trunks

CHAPTER CONTENTS

If you have analog or digital trunks, you need to configure those trunks in Wave before you can us them.

The base level configuration of the Wave IP 500 Server and Wave IP 2500 Server include two and four analog trunks respectively. Adding digital or additional analog trunks requires that the appropriate modules or cards be installed in the Wave Server. For more information, see the *Wave Server Installation Guide*.

This chapter describes the following tasks:

- Creating new trunk groups, if the default trunk groups provided with Wave do not meet your needs. You can rename the default trunk groups to be more meaningful to your business or call-routing scenarios, for example, Connect to PBX, Long Distance Calls, ISDN, and so forth.
- Modifying the default trunk groups to meet your specific requirements.
- Creating outside line-enabled trunk groups.
- Configuring trunks and channels.

Note: Before you configure trunk groups, trunks, and channels, be sure you understand the concepts presented in Chapter 27, Understanding Wave Trunks.

About creating new trunk groups

Before you can configure analog and digital trunks and put them in trunk groups, those trunk groups must exist. Wave provides default trunk groups (see the Default trunk groups table on page 27-5) that you can use to quickly group a set of analog or digital channels for most call routing scenarios.

If necessary, you can create additional trunk groups according to the steps in “Creating a new trunk group” on page 5-3. Those steps describe how to create, name, and set the direction and hunt order for a new trunk group. Later in the configuration process, you will configure Caller ID settings on the Out tab (see “Configuring Caller ID” on page 16-6) and configure the In tab (see “Configuring trunk groups for inbound call routing” on page 8-1).

About creating outside lines

You can map an Outside Line button on a digital phone directly to one or more trunks, simulating a key system.

Note: In Wave ISM, the term “outside line” specifically refers to this digital phone feature—throughout the Wave documentation, another term, “external line”, is used when referring to the common action of pressing a specific button (typically **9**) on any type of phone to get dial tone to make an external call.

Important! Calls made or answered via an Outside Line feature button on a phone do not appear in the ViewPoint Call Monitor because ViewPoint does not know about Outside Line feature button call activity.

Setting up outside lines consists of the following tasks:

- Create an outside line-enabled trunk group using the Trunk Groups applet.

  Note: One of the settings you specify when you create an outside line-enabled trunk group is whether it is a single-call variant or multiple-call variant outside line. The variant type determines how outside line buttons on digital phones are associated with the trunks in the trunk group. See page 29-27 for more about each variant type.

- Associate physical trunks with the outside line-enabled trunk group using the Trunk Configuration applet.

- Add Outside Line buttons to users’ digital phones in either of the following ways:
  - **User Configuration (Templates) applet.** Create or edit the feature button assignments in a digital phone template via the Feature Button Configuration dialog. Feature button assignments made via templates are applied to all users assigned that template. For details, see “Configuring phone templates” on page 10-2.
  - **User/Group Management applet.** Configure the phone features for an individual user’s digital phone via the User dialog Phone \ Station Features tab. Feature button assignments made via the Station Features tab apply only to that user’s phone. For details, see “The Phone \ Station Features tab” on page 11-72.

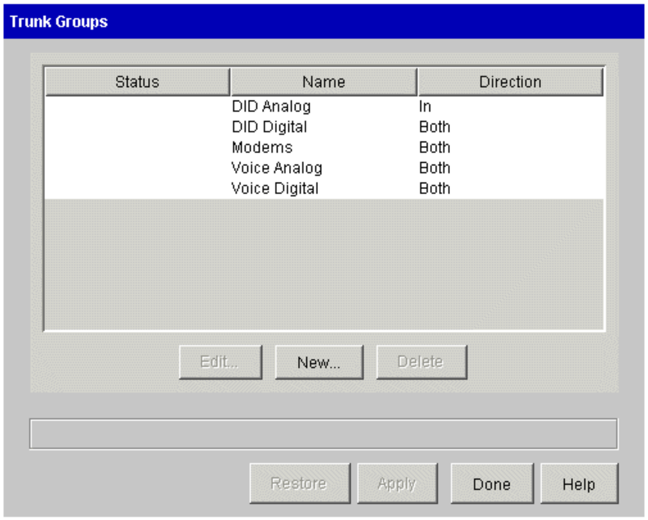
Creating a new trunk group

To create a new trunk group

1 If necessary, click the Administration tab of the Management Console.

Click

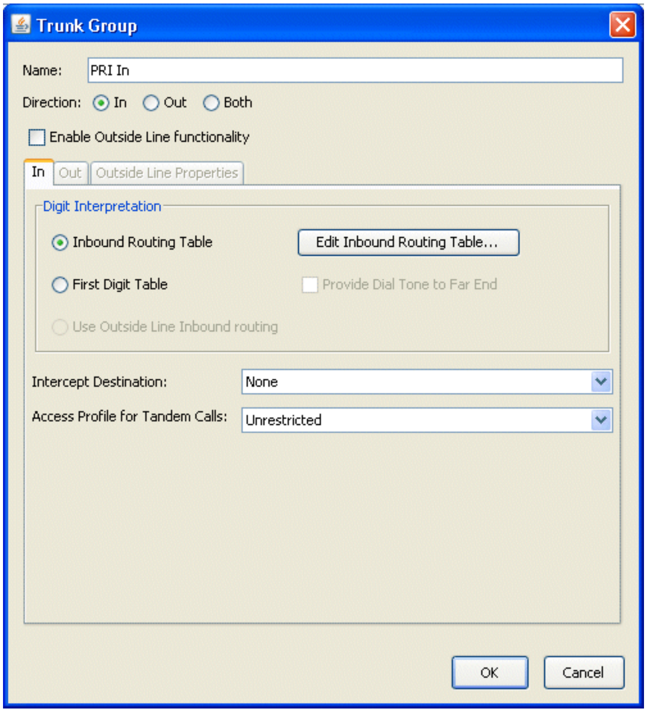
2 Click the Trunk Groups icon, located in the Trunk Administration section.



Trunk Groups

Status	Name	Direction
	DID Analog	In
	DID Digital	Both
	Modems	Both
	Voice Analog	Both
	Voice Digital	Both

3 Click **New** to create a new trunk group. The Trunk Groups dialog opens.



Trunk Group

Name: PRI In

Direction: ● In ○ Out ○ Both

□ Enable Outside Line functionality

Digit Interpretation

● Inbound Routing Table

○ First Digit Table

○ Use Outside Line Inbound routing

□ Provide Dial Tone to Far End

Intercept Destination: None

Access Profile for Tandem Calls: Unrestricted

4 At the top of the dialog, enter the following information:

- **Name**. Enter a name or phrase for the new trunk group, using up to 16 alphanumeric characters. This trunk group name will appear on Caller ID phones when calls are received via this trunk group and no Caller ID was received.

  Note: You can give a trunk group any meaningful or descriptive name. You might want to include “Trunk Group” in the name, for example “Voice Digital Trunk Group”, to differentiate trunk groups from routing tables that might have the same or similar names.

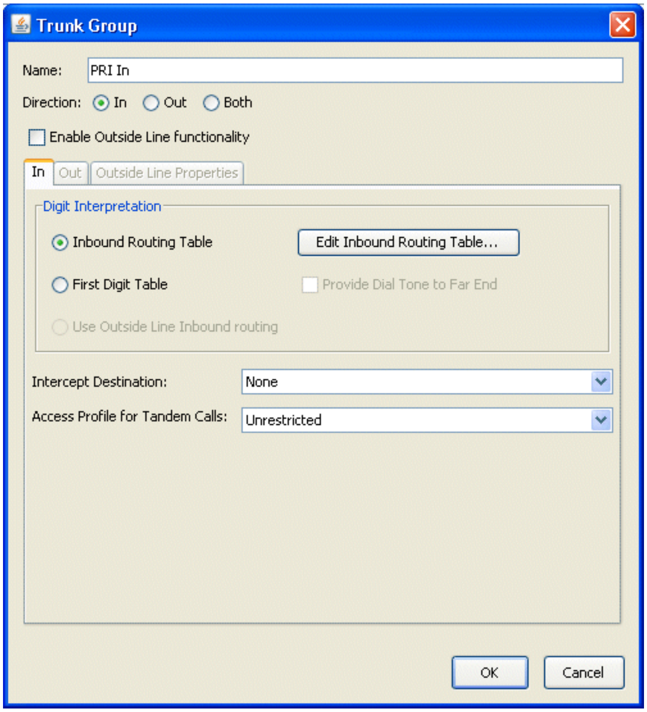
Hint: Wave automatically identifies an outside line-enabled trunk group when it displays the trunk group’s name in other applets (for example, Trunk Configuration) by prefixing the trunk group’s name with “OL|”. You may want to indicate in an outside line-enabled trunk group’s name whether it is a Single Call or Multiple Call variant outside line (selecting a variant is described in the following procedure.) This will make it easier later on to identify the trunk group and its qualities when you configure the trunks associated with the trunk group, via the Trunk Configuration applet.

- **Direction**. Select **In**, **Out**, or **Both** to specify the direction of the trunk group. Your Service Confirmation Letter should detail the direction of your installed trunks—refer to it to determine which direction to select here.

  Individual service providers may use different terms to describe trunk direction for voice circuits, for example:

  - “In”, “inbound” (with respect to the Wave Server)
  - “Out”, “outbound” (with respect to the Wave Server)
  - “Both”, “bidirectional”, “two-way”, “2-way”, “in and out”
- If you are configuring the trunk group with Outside Line functionality, select the **Enable Outside Line functionality** checkbox to create an outside line-enabled trunk group. Note that selecting this checkbox enables the Outside Line Properties tab as well as the **Use Outside Line Inbound Routing** setting on the In tab.

5 If this trunk group will be used for inbound calls, click the In tab to specify how inbound calls are to be handled.



Trunk Group

Name: PRI In

Direction: ● In ○ Out ○ Both

□ Enable Outside Line functionality

Digit Interpretation

● Inbound Routing Table

○ First Digit Table

□ Provide Dial Tone to Far End

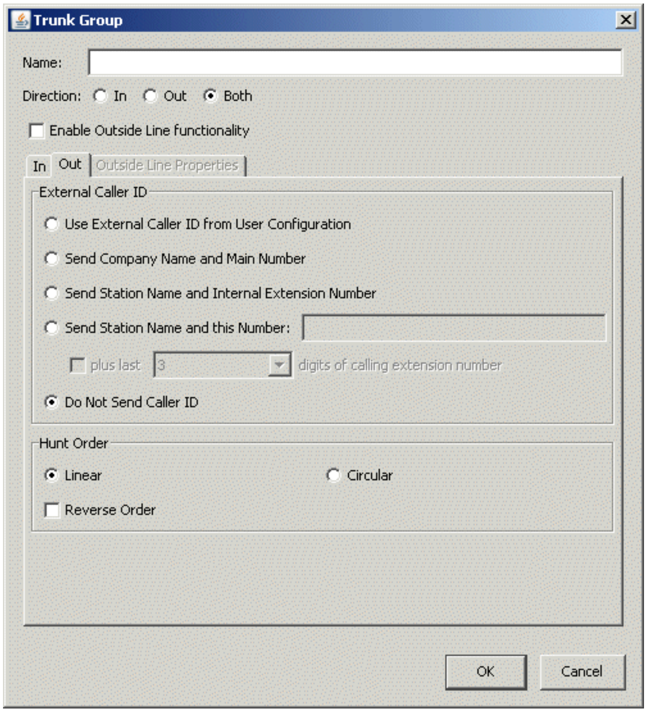
○ Use Outside Line Inbound routing

Intercept Destination: None

Access Profile for Tandem Calls: Unrestricted

See “Configuring trunk groups for inbound call routing” on page 8-1 for information on how to use the fields on this tab.

6 If this trunk group will be used for outbound calls, click the Out tab to specify how outbound calls are to be handled.



Trunk Group

Name:

Direction: ○ In ○ Out ● Both

□ Enable Outside Line functionality

In | Out | Outside Line Properties

External Caller ID

○ Use External Caller ID from User Configuration

○ Send Company Name and Main Number

○ Send Station Name and Internal Extension Number

○ Send Station Name and this Number:

□ plus last 3 digits of calling extension number

● Do Not Send Caller ID

Hunt Order

● Linear ○ Circular

□ Reverse Order

7 In the External Caller ID section, specify how to provide Caller ID for outbound calls:

- **Use External Caller ID from User Configuration**. Select this option to send the information specified for the user as entered in the User/Group Management applet. (Unless modified for an individual user, this will be the default information specified in the General Settings applet.)
- **Send Company Name and Main Number**. Select this option to send the **Company Name** and **Main Number**, as entered in the System tab of the General Settings applet.

  Note: Although **Company Name** can include up to 16 alphanumeric characters, be aware that no more than 15 Caller ID characters can be sent over an ISDN trunk.

- **Send Station Name and Internal Extension Number**. Select this option to send the Station Name, as entered in User/Group Management applet.
- **Send Station Name and this Number**. Select this option to send the Station Name (as entered in User/Group Management applet) followed by the digits you enter. (Use this setting to provide station name and number on outbound calls.)

  In addition, if you select the **plus last ___ digits of calling extension number** checkbox, the specified number of digits from the calling extension are appended to the digits you entered.

- **Do Not Send Caller ID**. Select this option if you do not want to provide external Caller ID.

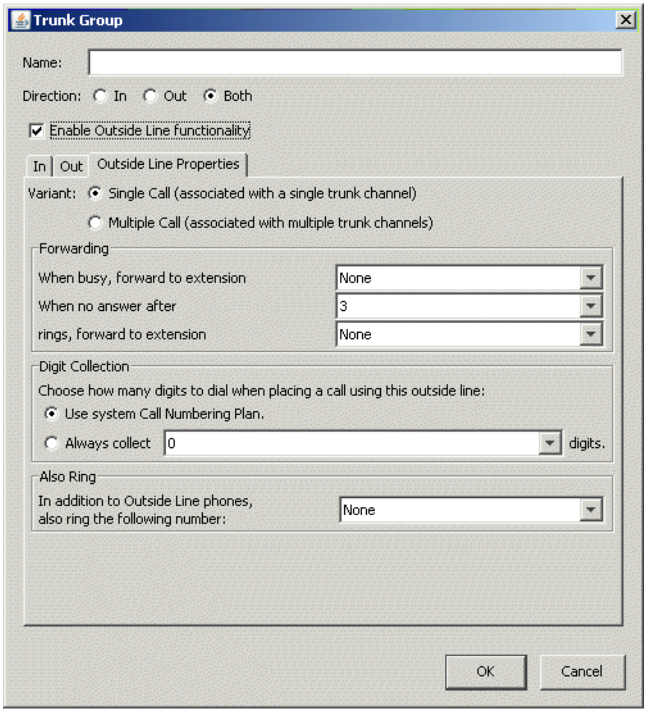
8 In the Hunt Order section, select one of the following:

- **Linear.** Looks for a free channel, always starting at the beginning of the list of trunks in the trunk group and searching to the end, or—for reverse-order hunting—always starting at the end of the list and searching to the beginning.
- **Circular.** Looks for a free channel, starting where the last search left off. From this point (where the last search left off), forward-order hunting works forward through the list of available channels, and reverse-order hunting works backward through the list.

  For either hunt order type, select the **Reverse Order** checkbox as applicable.

For more information about hunt order types, see “Trunk group hunt types” on page 27-7.

9 If you selected **Enable Outside Line functionality** to create an outside line-enabled trunk group, click the Outside Line Properties tab.



Trunk Group

Name:

Direction: ○ In ○ Out ● Both

☑ Enable Outside Line functionality

In | Out | Outside Line Properties

Variant: ● Single Call (associated with a single trunk channel)
○ Multiple Call (associated with multiple trunk channels)

Forwarding
When busy, forward to extension: None
When no answer after 3 rings, forward to extension: None

Digit Collection
Choose how many digits to dial when placing a call using this outside line:
● Use system Call Numbering Plan.
○ Always collect 0 digits.

Also Ring
In addition to Outside Line phones, also ring the following number: None

10 Specify the **Variant**, one of two ways in which outside line buttons on digital or SIP phones will be associated with the trunks in this trunk group:

- **Single Call**. Select this option (the default) to associate each outside line with a single trunk. If lit, the light next to the outside line button on a user's digital phone indicates if the trunk is in use by any phone.
- **Multiple Call**. Select this option to associate each outside line with multiple trunks. If lit, the light next to the outside line button on a user's digital phone indicates if all of the associated trunks are in use.

Warning: *Once you select a **Variant** and click **Apply** or **Done** in this dialog, if you want to change the variant you must first deselect the **Enable Outside Line functionality** checkbox, click **Apply**, make the change, and then re-select **Enable Outside Line functionality**.*

For more about Single Call and Multiple Call variants, see "Outside lines" on page 29-27.

11 In the Forwarding section, specify the forwarding options to be applied to inbound calls on this outside line:

- **When busy, forward to extension**. Select the extension to which an inbound call will be forwarded when all associated outside line buttons are busy with other calls. If you select **None** (the default), the caller will hear a busy signal.
- **When no answer after**. Select the number of rings (up to 9) to wait before forwarding an unanswered inbound call to the extension specified in the next field.
- **rings, forward to extension**. Select the extension to which an unanswered inbound call will be forwarded after the number of rings specified in the previous field. If you select **None** (the default), associated phones will ring indefinitely.

12 In the Digit Collection section, choose how many digits to dial when placing outbound calls on this outside line:

- **Use system Call Numbering Plan**. Select this option so that the system will determine how many digits to wait for depending on the first digits dialed. For example, under the North American Numbering Plan, if a user dials a 1, the system waits for 10 more digits before sending the number to the central office.
- **Always collect __ digits**. Select this option to require the user to enter the specified number of digits when placing a call on the outside line.

13 In the Also Ring section, select any extension or station hunt group to be rung along with associated digital phones on an inbound call.

14 When you are done creating or editing the trunk group, click **OK** to save your changes and close the Trunk Group dialog.

15 Click **Done** to close the Trunk Groups applet and return to the Management Console.

Deleting a trunk group

You cannot delete a trunk group that is still in use in the current configuration. If you attempt to do so, Wave identifies the conflicts that must be resolved before you can complete the deletion.

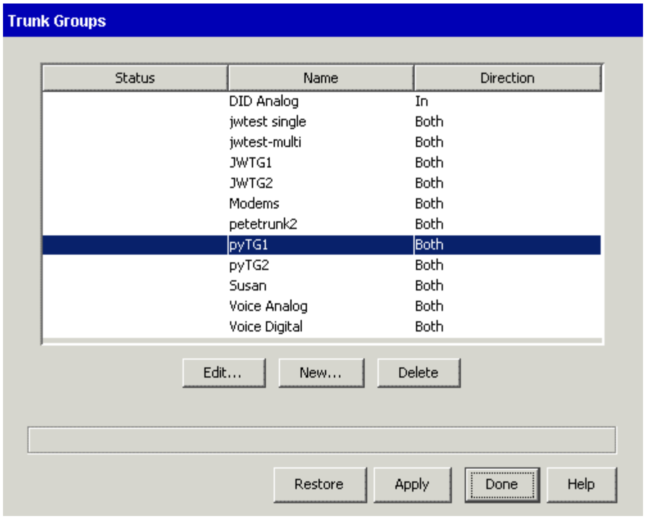
To delete a trunk group

1 If necessary, click the Administration tab of the Management Console.

Click

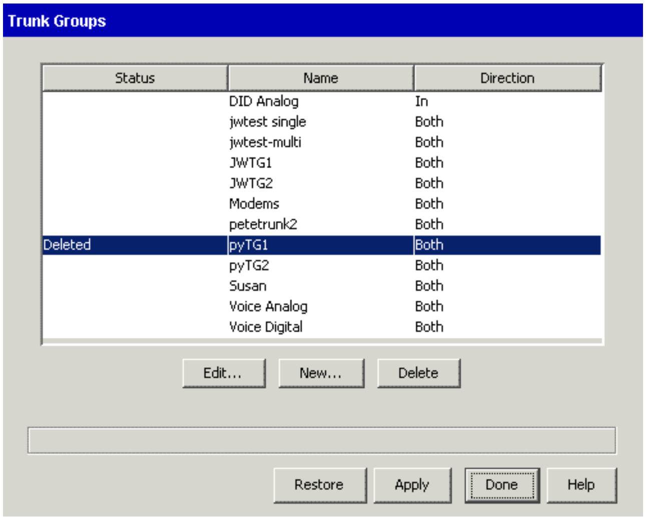
2 Click the Trunk Groups icon, located in the Trunk Administration section.

3 Select one or more trunk groups and then click **Delete**.



Status	Name	Direction
	DID Analog	In
	jwtest single	Both
	jwtest-multi	Both
	JWTG1	Both
	JWTG2	Both
	Modems	Both
	petetrunk2	Both
	pyTG1	Both
	pyTG2	Both
	Susan	Both
	Voice Analog	Both
	Voice Digital	Both

4 The **Status** for the Trunk Group changes to Deleted.

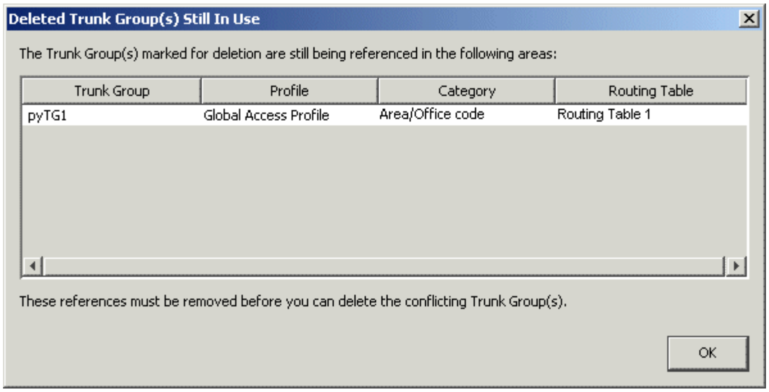

Trunk Groups

Status	Name	Direction
	DID Analog	In
	jwtest single	Both
	jwtest-multi	Both
	JWTG1	Both
	JWTG2	Both
	Modems	Both
	petetrunk2	Both
Deleted	pyTG1	Both
	pyTG2	Both
	Susan	Both
	Voice Analog	Both
	Voice Digital	Both

5 When you have no further changes to make in the Trunk Groups applet, click **Done**. Click **Yes** when you asked if you want to save your changes.

6 If any conflicts are detected, you will observe the following depending on where the conflict exists:

- **If the trunk group you selected is still in use in the Outbound Routing applet**, the Deleted Trunk Group(s) Still In Use dialog opens, listing the locations where the trunk group is still being used.


Deleted Trunk Group(s) Still In Use

The Trunk Group(s) marked for deletion are still being referenced in the following areas:

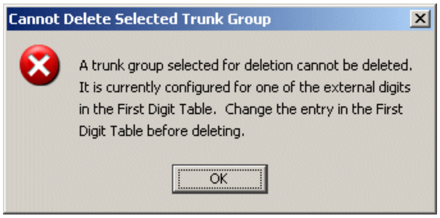
Trunk Group	Profile	Category	Routing Table
pyTG1	Global Access Profile	Area/Office code	Routing Table 1

These references must be removed before you can delete the conflicting Trunk Group(s).

The following information is displayed for each conflict:

- **Trunk Group**. Name of the trunk group that is still in use.
- **Profile**. Access profile name where the hunt group is used, for example “Global Access Profile”, “Private Network”, or custom access profile name.
- **Category**. Category within the access profile, for example Area Code Table, Off-Premise Extension Table, Special Digits Table, Privileges, and so forth.
- **Routing Table**. Name of the routing table where the conflict exists, or “None” for Privileges or Carrier Access.

- **If the trunk group you selected is still configured for one of the external digits in the First Digit Table**, the Cannot Delete Selected Trunk Group dialog opens:



Cannot Delete Selected Trunk Group

A trunk group selected for deletion cannot be deleted. It is currently configured for one of the external digits in the First Digit Table. Change the entry in the First Digit Table before deleting.

Important! Make a note of the conflicts so that you can address all of them. The trunk group in question cannot be deleted until all outstanding conflicts have been resolved.

7 Click **OK**. The Trunk Groups applet closes automatically. In the Outbound Routing applet, remove the trunk group in question from the configuration to resolve all identified conflicts. Then run the Trunk Groups applet again and delete the trunk group.

Configuring trunks and channels

You use the Trunk Configuration applet to set up the handshake and signaling between the Wave Server and the equipment on the service provider end of the trunk. Using this applet, you can set the configuration options to match the settings your trunk service provider has provisioned on your trunks.

Locate your Service Confirmation Letters or provisioning information forms before starting the following procedures. See “Sample trunk service confirmation letter” on page C-3 for an example.

Caution! *The trunk options and the channel/trunk signaling options must be set identically to the settings shown on your trunk Service Confirmation Letter.*

Caution! *Never mix trunk types within a trunk group. If necessary, create a new trunk group (see “About creating new trunk groups” on page 5-2).*

Trunk and channel settings

Both digital channels and analog trunks have three major configuration parameters, as described in the following table:

Parameter Name	Description
Enabled	Places a T-1 or analog channel or trunk into service or removes it from service.
Signaling	Sets the signaling method for the channel or trunk.
Trunk group (for voice or modem channels)	Sets the trunk group membership for the analog trunks or digital channels. For example, you can assign a trunk group called Voice Analog to eight separate analog trunks.

Configuring analog trunks

You use the Trunk Configuration applet to configure analog trunk settings for the analog trunk ports on the Integrated Services Card or on expansion cards and modules. Refer to your Service Confirmation Letter, provided by your service provider, for the appropriate values to set.

Before configuring the trunks, configure the trunk groups you want to assign to the analog trunks. For information about configuring trunk groups, see “About creating new trunk groups” on page 5-2.

Caution! *If you need to permanently remove an analog trunk module from your Wave Server, or replace an analog trunk module with a different module, you must first assign all ports of the module to None in the Trunk Group drop-down list in the Trunk Configuration applet. For details about this drop-down list, see step 5 of “Configuring analog channels” on page 5-17.*

Complete the following tasks to configure analog trunks:

- Configuring analog trunk card or module settings
- Configuring analog channels

This section also describes how to customize AC impedance settings on analog trunk ports in order to correct echo return loss problems. See page 5-19.

Using analog loop start trunks with mobile extensions

Using mobile extensions over trunks which do not support disconnect supervision can cause a trunk to get stuck, requiring you to disable and re-enable the trunk via the Trunk Configuration applet. This problem can occur when a user on a mobile extension connected via an analog loop start trunk puts a call on hold and goes onhook. The problem stems from the fact that the CO does not always propagate disconnects over loop start trunks, so Wave is never informed when the user goes onhook.

It is highly recommended that all analog trunks be tested for disconnect supervision by calling an external number from a Wave phone, connecting, and then having the called (external) party hang up. If the Trunk Monitor indicates that the trunk cleared before the local extension went onhook, then the trunk does support disconnect supervision and can be safely used for mobile extensions. For more about mobile extensions, see “Using mobile extensions for externally routed calls” on page 11-63.

Configuring analog trunk card or module settings

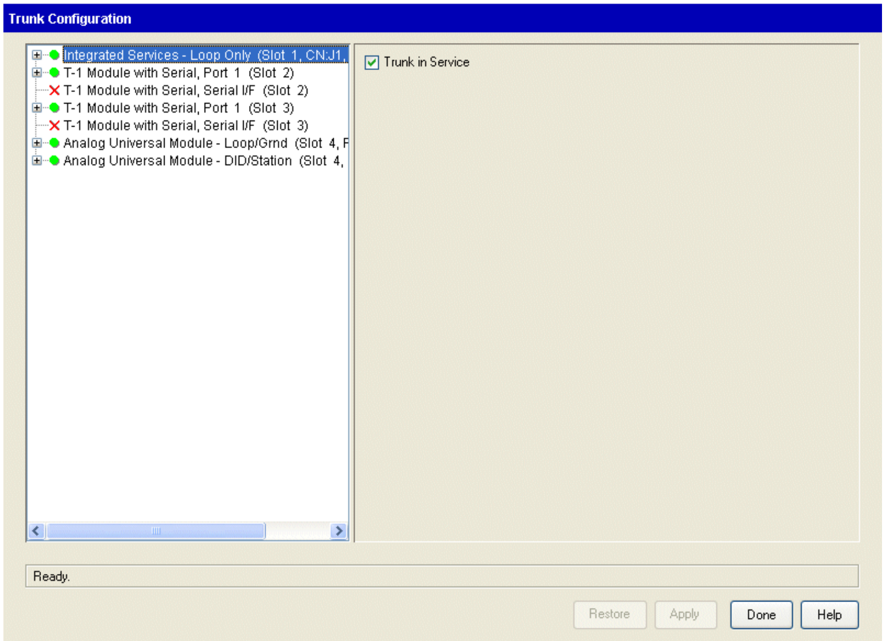
To configure the analog trunk card or module settings

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Select the card or module you want to configure, then select the **Trunk in Service** check box.



Trunk Configuration

- Integrated Services - Loop Only (Slot 1, CN:J1,
- T-1 Module with Serial, Port 1 (Slot 2)
- T-1 Module with Serial, Serial I/F (Slot 2)
- T-1 Module with Serial, Port 1 (Slot 3)
- T-1 Module with Serial, Serial I/F (Slot 3)
- Analog Universal Module - Loop/Grnd (Slot 4, F
- Analog Universal Module - DID/Station (Slot 4,

☑ Trunk in Service

Ready.

Note: If your Wave Server only has a Integrated Services Card and no other analog trunk modules, there will only be one entry in the list, **Integrated Services Card - Loop Only**.

Refer to the *Wave Server Hardware Reference Guide* for information about each card and module installed in your Wave Server.

4 Configure the card or module’s analog trunks or ports, which are called channels (see “Configuring analog channels” on page 5-17).

5 Click **Apply** to save your changes.

6 Click **Done** to return to the Management Console.

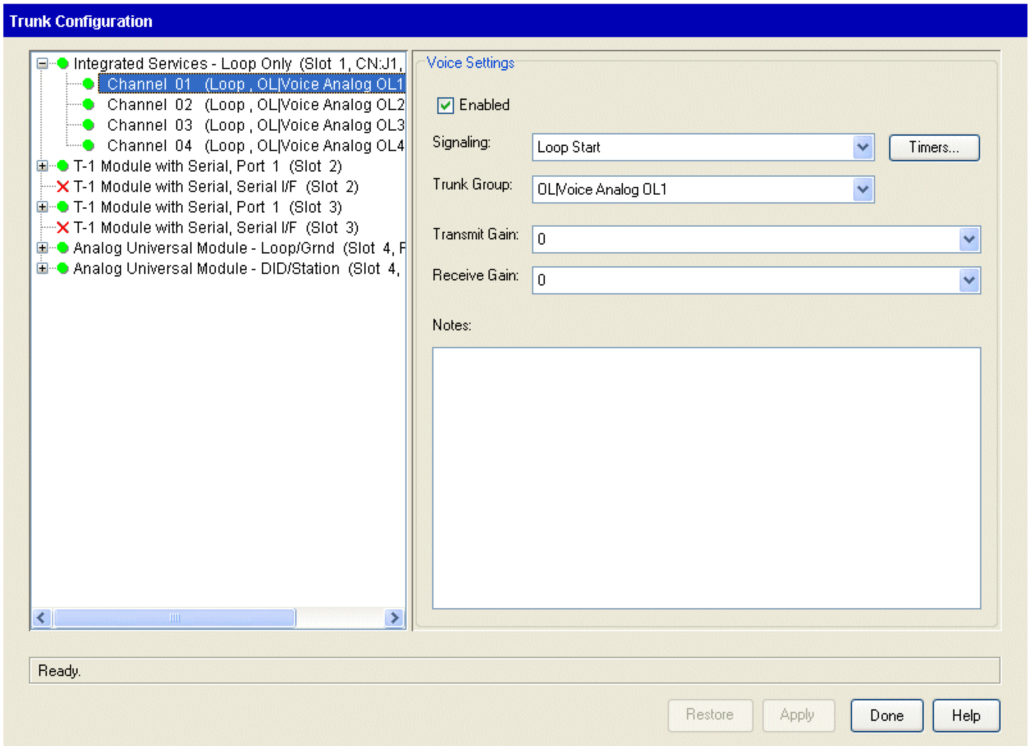
Configuring analog channels

To configure a card or module’s analog channels

1 Select the card or module according to the steps in “Configuring analog trunk card or module settings” on page 5-16.

2 Click the + next to a card or module to display the channels, and select the channels you want to configure.

- To select a contiguous range of channels, select the first channel in the range, then hold down the Shift key while you select the last channel in the range.
- To select a noncontiguous range of channels, hold down the Ctrl key while you select each channel.


Trunk Configuration

- Integrated Services - Loop Only (Slot 1, CN:J1,
  - Channel 01 (Loop , OL|Voice Analog OL1
  - Channel 02 (Loop , OL|Voice Analog OL2
  - Channel 03 (Loop , OL|Voice Analog OL3
  - Channel 04 (Loop , OL|Voice Analog OL4
- T-1 Module with Serial, Port 1 (Slot 2)
- T-1 Module with Serial, Serial I/F (Slot 2)
- T-1 Module with Serial, Port 1 (Slot 3)
- T-1 Module with Serial, Serial I/F (Slot 3)
- Analog Universal Module - Loop/Grnd (Slot 4, F
- Analog Universal Module - DID/Station (Slot 4,

Voice Settings

☑ Enabled

Signaling: Loop Start

Trunk Group: OL|Voice Analog OL1

Transmit Gain: 0

Receive Gain: 0

Notes:

Ready.

3 Make sure that the channels are enabled—to do so, select the **Enabled** check box.

4 Select the signaling method from the **Signaling** drop-down list.

The signaling method is indicated on your Service Confirmation Letter. See “Sample trunk service confirmation letter” on page C-3 for an example.

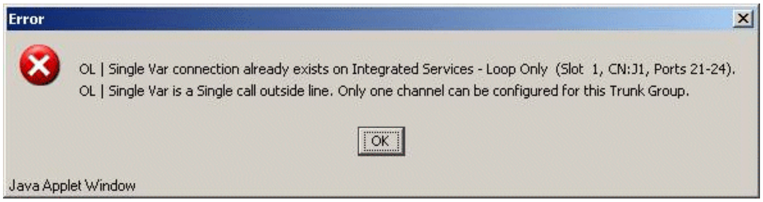
The signaling methods are as follows:

- **Loop Start.** This option is required if you are configuring the analog trunks on the Integrated Services Card.
- **Ground Start.** This option is available only for the Analog Universal Module and the Analog Trunk Module.
- **Wink Start**. This option is available only for the Analog Universal Module.

Caution! *Timer settings (accessed via the Timers button) are expert settings, and should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

5 Select the trunk group you want to assign to the selected trunks from the **Trunk Group** drop-down list.

Warning: *If the trunk group you select is a Single Call variant outside line-enabled trunk group and you had previously selected more than one channel in step 2, you will see an error message similar to the following. Click OK to clear the message, and go back and select a single channel:*


Error

OL | Single Var connection already exists on Integrated Services - Loop Only (Slot 1, CN:J1, Ports 21-24).
OL | Single Var is a Single call outside line. Only one channel can be configured for this Trunk Group.

6 Adjust the Transmit Gain and Receive Gain values if necessary.

- **Transmit Gain**. If the voice level of outgoing calls is too low, increase the value; if the voice level is too high, decrease the value.
- **Receive Gain**. If the voice level of incoming calls is too low, increase the receive gain; if the voice level is too high, decrease the value.

Caution! *Feedback can result if you set the gain level too high. In most cases, the default value of 0 should be fine.*

7 Record information in the Notes field.

This information could include circuit-specific information or other information from the Trunk Configuration property sheet. Circuit number and carrier information or brief notes regarding issues encountered can be entered in this comment field. Field personnel can use this data to locate and identify the physical circuit connected to the Wave Server.

8 Click **Apply** to save your changes.

9 Click **Done** to return to the Management Console.

Customizing AC impedance settings on analog trunk ports

You can customize AC impedance settings on analog trunk ports in order to correct echo return loss problems. In cases where the echo return loss is poor, users may experience unusually loud side-tone or echo on calls over analog trunks.

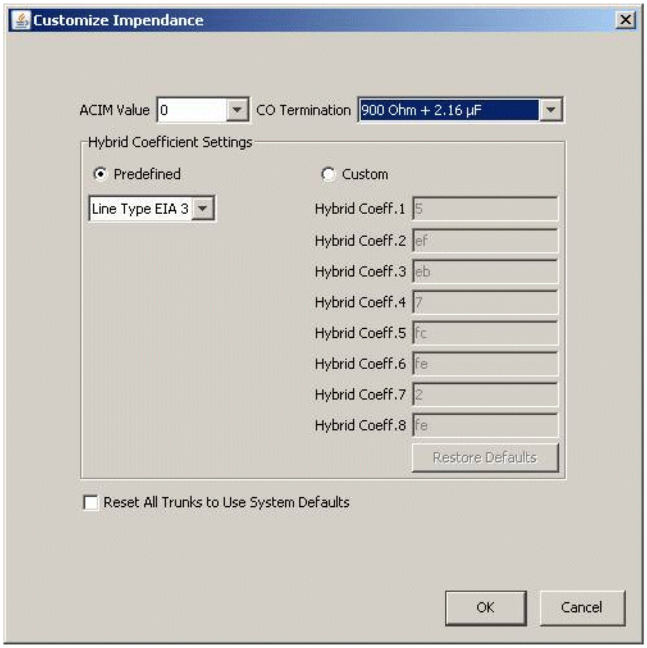
Caution! *These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative in order to resolve a specific analog trunk echo problem. Improper settings will degrade voice quality on calls.*

To customize AC impedance settings

1 There are 2 ways to configure AC impedance settings for analog trunks:

- **Via the General Settings applet**. Use this method to customize AC impedance settings for all analog trunks, as part of the system Locale settings. On the System tab click **Customize**. When the Customize Locale dialog opens, click **Analog Trunk Impedances**.
- **Via the Trunk Configuration applet**. Use this method to customize AC impedance settings for specific analog trunks or channels. In the Trunk Configuration dialog, select one or more analog channels and then click **Impedance**.

In both cases, the Customize Impedance dialog opens.



Customize Impendance

ACIM Value: 0

CO Termination: 900 Ohm + 2.16 µF

Hybrid Coefficient Settings

● Predefined ○ Custom

Line Type EIA 3

Hybrid Coeff.1: 5

Hybrid Coeff.2: ef

Hybrid Coeff.3: eb

Hybrid Coeff.4: 7

Hybrid Coeff.5: fc

Hybrid Coeff.6: fe

Hybrid Coeff.7: 2

Hybrid Coeff.8: fe

□ Reset All Trunks to Use System Defaults

Depending on how you accessed this dialog, different default values will be displayed:

- From the Customize Locale dialog, the defaults reflect valid combinations of pre-defined data for the selected Locale.
- From the Trunk Configuration applet, pre-defined system values are displayed.

2 Specify the following information:

- **ACIM Value**. Specifies the terminating impedance that Wave analog trunks present to the CO. **ACIM Value** is location-specific and generally does not need to be changed.

  For North America, the correct value is 0, which sets the Wave trunk terminating impedance to 600 Ohms. Other locale-specific defaults may have different values.

  Note: This value is not the same as the value displayed in the CO Termination field.

- **CO Termination**. Specifies the terminating impedance that the CO presents to Wave trunk. **CO Termination** is associated with the **ACIM Value** and generally does not need to be changed.

  For some locations, there may be an alternate value that can be tried. In North America the terminating impedance presented by the CO is 900Ohms + 2.16uF. In North America the alternate CO Termination value is 600 Ohms. This alternate choice may sometimes apply if Wave is connected to a local PBX rather than directly to the CO—some PBXs provide a 600 Ohm terminating impedance instead of the standard 900ohms+2.16uF presented by the CO.
- **Predefined/Custom**. Select one of the following:
  - **Predefined**. Select this option to use the default hybrid coefficients based on the selected **ACIM Value** and **Line Type**. In almost all cases, this will result in acceptable performance.
  - **Custom**. Select this option to define alternative hybrid coefficients in rare cases where adequate performance cannot be obtained via a predefined **Line Type**.

  Caution! *Identifying custom hybrid coefficient values should only be done under the direction of your Vertical Technical Support representative.*
- **Line Type**. Specifies the length and characteristics of the 2-wire cable that connects the Wave Server to the CO. There are 8 predefined EIA line types, EIA 0 – EIA 7:
  - EIA 0 represents the shortest cable length (under 2000 feet).
  - EIA 6 and EIA 7 represent the longest and most complex line types.

  Note: Testing has shown that EIA 3 is an appropriate setting for most installations. In cases where EIA 3 is does not provide good performance, one of the other predefined EIA line types can usually be found to provide adequate echo return loss performance.
- **Hybrid Coeff.1 - 8**. If you selected **Custom** above, enter a value from 0-255 in the text box for a specific hybrid coefficient. Click **Restore Defaults** to discard your changes and restore the default values.

3. To discard all of your changes and revert to the pre-defined system values, select the **Reset All Trunks to Use System Defaults** checkbox.
4. Click **OK**.

Configuring digital trunks and channels

You use the Trunk Configuration applet to assign voice, data, or ISDN traffic to digital channels; to configure connection settings for a digital channel on WAN modules or cards (for example, the two-port T-1 module); and to assign each channel to a connection.

Caution! *If you need to remove a T-1 module from the Wave Server, you must first assign all channels of the module to None in the Connection drop-down list in the Trunk Configuration applet. For details about this drop-down list, see "Configuring digital trunk card or module settings," step 5.*

See the following sections to configure digital channels:

- Configuring digital trunk card or module settings. See page 5-23.
- Configuring digital channels. See page 5-30.
- Configuring digital channels for voice. See page 5-31.
- Configuring digital channels for data. See page 5-34.
- Configuring digital channels for ISDN. See page 5-35.
- Assigning digital channels to a serial interface. See page 5-36.
- Configuring ports and channels on the Quad BRI Module. See page 5-37.

After making changes to your digital trunk configuration

Note the following:

- **Courtesy vs. Forced reset:** Some digital trunk and digital channel configuration changes require that you reset the affected trunks or channels for the changes to take effect. When this occurs, you are prompted to perform either a Courtesy or Forced reset.

  At the digital trunk level:

  - **If you choose a Courtesy reset**, changes are applied immediately if the trunk is idle. If the trunk is not idle, calls in progress are allowed to complete, but all new inbound and outbound calls on the entire span are blocked. When the entire span is idle (which may take awhile on a busy system), your changes will be applied.
  - **If you choose a Forced reset**, changes are applied immediately. Any active calls are disconnected, and all new inbound and outbound calls on the trunk are blocked until the trunk is reset.

At the digital channel level:

  - **If you choose a Courtesy reset**, changes are applied immediately if the channel is idle. If the channel is not idle, calls in progress are allowed to complete, but all new inbound and outbound calls on the channel are blocked. When the channel is idle, your changes will be applied.
  - **If you choose a Forced reset**, changes are applied immediately. Any active calls are disconnected, and all new inbound and outbound calls on the channel are blocked until the channel is reset.

- After installing a digital trunk module in a Wave Server and configuring the trunks and channels on the module, trunks and channels on existing digital trunk modules may go offline. To resolve this issue, do the following:

  a Edit one of the affected existing digital trunks via the Trunk Configuration applet.

  b Select the channels on the trunk.

  c Deselect the **Enabled** checkbox, and then click **Apply**.

  d Select the **Enabled** checkbox again, and then click **Apply**.

  e Repeat these steps for on any other affected digital trunk modules.

Configuring digital trunk card or module settings

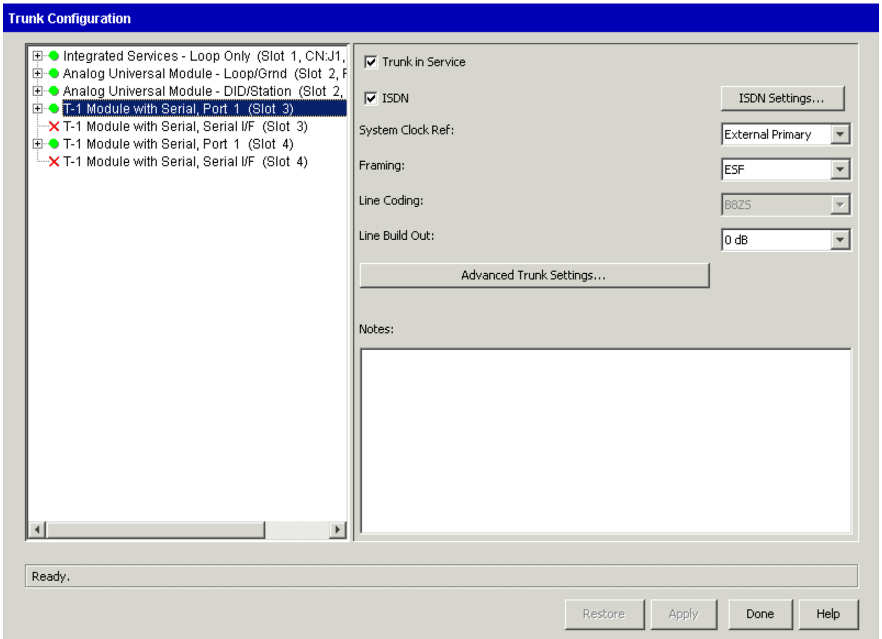
To configure the digital trunk card or module settings

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Select the digital card or module you want to configure, and select the **Trunk In Service** check box.



Trunk Configuration

- ⊞ ● Integrated Services - Loop Only (Slot 1, CN:J1,
- ⊞ ● Analog Universal Module - Loop/Grnd (Slot 2, F
- ⊞ ● Analog Universal Module - DID/Station (Slot 2,
- ⊞ ● T-1 Module with Serial, Port 1 (Slot 3)
- ✕ T-1 Module with Serial, Serial I/F (Slot 3)
- ⊞ ● T-1 Module with Serial, Port 1 (Slot 4)
- ✕ T-1 Module with Serial, Serial I/F (Slot 4)

☑ Trunk in Service

☑ ISDN

System Clock Ref: External Primary

Framing: ESF

Line Coding: B8ZS

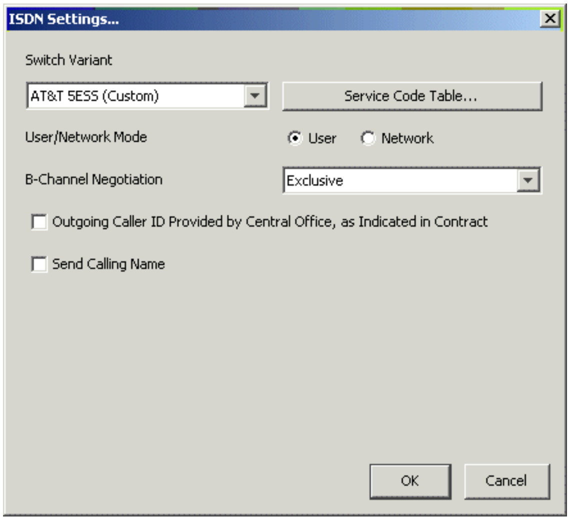
Line Build Out: 0 dB

Notes:

Ready.

Note: If you want to configure a module for cross-connection to a serial interface, Be sure that you select the module labeled “Serial”.

4 If the trunk is ISDN, check the **ISDN** check box, and click **ISDN Settings** to configure the ISDN trunk settings as follows:



ISDN Settings...

Switch Variant: AT&T 5ESS (Custom)

User/Network Mode: ● User ○ Network

B-Channel Negotiation: Exclusive

□ Outgoing Caller ID Provided by Central Office, as Indicated in Contract

□ Send Calling Name

Note: If you do not select the **ISDN** check box, the trunk will be a CAS (Channel Associated Signaling) T-1 trunk, which implies robbed-bit signaling or clear channel for data. Clear channels (whether ISDN or CAS) must be assigned to data connections, and channels grouped for data connections must be contiguous. All other channel types, like B channels, must be assigned to voice trunk groups. If you configure ISDN to use a voice trunk group, you can configure that ISDN connection for dial-up data; see “Configuring dial-up routing” on page 21-1.

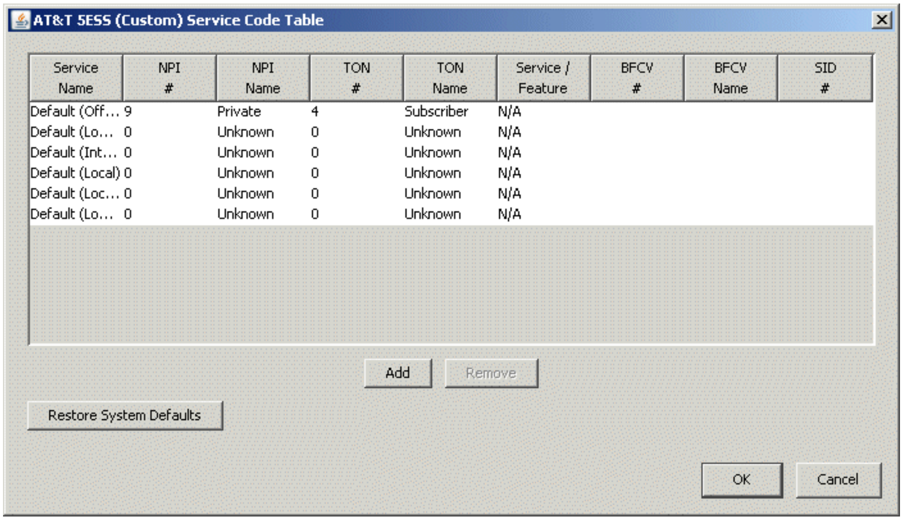
a Select a variant in the **Switch Variant** drop-down list.

Refer to your T-1 Service Confirmation Letter to determine which of the following ISDN switch variants to use:

- AT&T 5ESS (Custom)
- AT&T 4ESS
- NT DMS-100 (NI-1)
- AT&T 4ESS (NI-2)
- NT DMS-100 /S-100

Select the NT DMS-100 /S-100 variant when connecting to a Northern Telecom Meridian DMS-100 PBX configured with a subtype profile of S-100. In this scenario, the DMS-100 must be configured as the network side. Wave is always the user side.

b Click **Service Code Table** to modify the service code table for the switch variant that you specified in the previous step.



AT&T 5ESS (Custom) Service Code Table

Service Name	NPI #	NPI Name	TON #	TON Name	Service / Feature	BFCV #	BFCV Name	SID #
Default (Off...	9	Private	4	Subscriber	N/A			
Default (Lo...	0	Unknown	0	Unknown	N/A			
Default (Int...	0	Unknown	0	Unknown	N/A			
Default (Local)	0	Unknown	0	Unknown	N/A			
Default (Loc...	0	Unknown	0	Unknown	N/A			
Default (Lo...	0	Unknown	0	Unknown	N/A			

Note: You do not need to modify the service code table during initial configuration. The defaults should be sufficient for connecting to a local exchange carrier.

c If your ISDN trunks support multiple services, click **Add** to add new service name records to the service code table, then modify the new records by clicking in each field to open a text field or a drop-down list.

Note: The new entries in the service code table appear as ISDN Setting options in the outbound routing tables. You will configure the outbound routing tables in "Configuring outbound routing tables" on page 9-20. You can select these settings on a call-by-call basis.

You can modify the following fields for new entries and existing entries:

- **Service Name**. A text string, such as OUTWATS, FX, TIE, VNET
- **NPI #**. Numbering Plan Identifier, 0 through 15.
  - **0** = unknown, the network has no knowledge of the numbering plan so it uses the NANP.
  - **1** = ISDN/telephony number plan. Enter the name `E.164` in the NPI Name field.
  - **9** = private numbering plan (private network).

- **NPI Name**. A text string describing the Numbering Plan Identifier; typically E.164, Unknown, or Private.
- **TON #**. Type of Number. There can only be four different types of entries:
  - **0** = unknown.
  - **1** = international number.
  - **2** = national number.
  - **4** = subscriber number.
- **TON Name**. A text string describing the Type of Number; typically National, International, or Unknown.
- **Service/Feature**. Service vs. Feature. Typically left N/A unless the provider states that it should be either Service or Feature.
- If you select Service or Feature, you need to configure the next three settings:

  BFCV #. Binary Facility Coding Value, 0 through 31.

  A number for the service must be entered in the BFCV field. The provider provides this number. The number can be from 0 through 31.

  Some common Service IDs:

  - **1** = SDN (including GSDN) = in/out.
  - **2** = Toll free MEGACOM= in.
  - **3** = MEGACOM = out.
  - **6** = ACCUNET Switched Digital Service = in/out.
  - **7** = Long Distance Service = in/out.
  - **8** = International Toll Free Service = in.
  - **10** = ATT MultiQuest = in.
  - **17** = Call Redirection Service = in.

  BFCV Name. A text string describing the BFCV value.

  SID #. Service Identifier, 0 through 127. Used primarily by Bell Canada.

  If you are not sure of your changes, click **Restore System Defaults** to restore your changes to the system defaults.

d Select the appropriate mode.

- **User**. This is the typical setting, unless you are connecting two Wave Servers together.
- **Network.** Use this setting if you are connecting two Wave Servers together. In this case, one Wave Server must be set to User and the other set to Network.

Caution! *These settings should not be adjusted unless you are instructed to do so by your Vertical Technical Support representative.*

e Select the **Outgoing Caller ID Provided by Central Office** check box if your contract specifies that the central office will provide Caller ID.

In this case, the central office will typically provide the ISDN trunk's billing number as Caller ID for all outgoing calls.

To configure ISDN channel settings, see "Configuring digital channels for ISDN" on page 5-35.

f Check the **Send Calling Name** check box if you want Wave to send the name specified in the General Settings applet when calls are sent over this trunk.

5 Specify the system clock reference in the **System Clock Ref** drop-down list. Available options are:

- **Internal**. The selected T-1 trunk will not be a clock reference source for the Wave Server, rather, the selected T-1 will act as a clock reference for the equipment connected to the T-1 trunk. This is useful if the Wave Server is to be master clock to another Wave Server or internal device. In this case, the other device should be configured as External.
- **External Primary**. The Wave Server gets its primary clock reference from the selected T-1 trunk. Use this for a T-1 trunk connecting to the PSTN. Only one trunk can be primary.
- **External Secondary**. If the primary T-1 trunk fails, the Wave Server will get its primary clock reference from the secondary T-1. Only one trunk can be secondary.

Note: If you configure one trunk as secondary, the other trunk must be primary. If you have only one T-1 connection between your Wave Server and the PSTN, that connection must be the primary one. If you have two T-1s connected, the connection you are using for voice must be the primary one, and the other (typically set for data use) is secondary.

6 Set the following fields using the information on your T-1 Service Confirmation Letter.

- **Framing.** ESF (Extended Super Frame) or SF/D4 (Super Frame - D4). ISDN PRI is generally ESF.
- **Line Coding.** B8ZS (Bipolar 8 Zero Substitution) or AMI (Alternate Mark Inversion). ISDN PRI is B8ZS; AMI is not supported for ISDN.
- **Line Build Out.** 0 dB, -7.5 dB, -15 dB, and -22.5 dB are available if DSX mode is selected in Advanced Trunk Settings. Otherwise, in CSU mode, 0, -7.5, and -15 are available. (For details about line build out settings, see “Line Build Out settings” on page 34-1)

7 Record information in the **Notes** field. This information could include circuit specific information or other information from the Trunk Configuration property sheet. Circuit number and carrier information or brief notes regarding issues encountered can be entered in this comment field. Field personnel can use this data to locate and identify the physical circuit connected to the Wave Server.

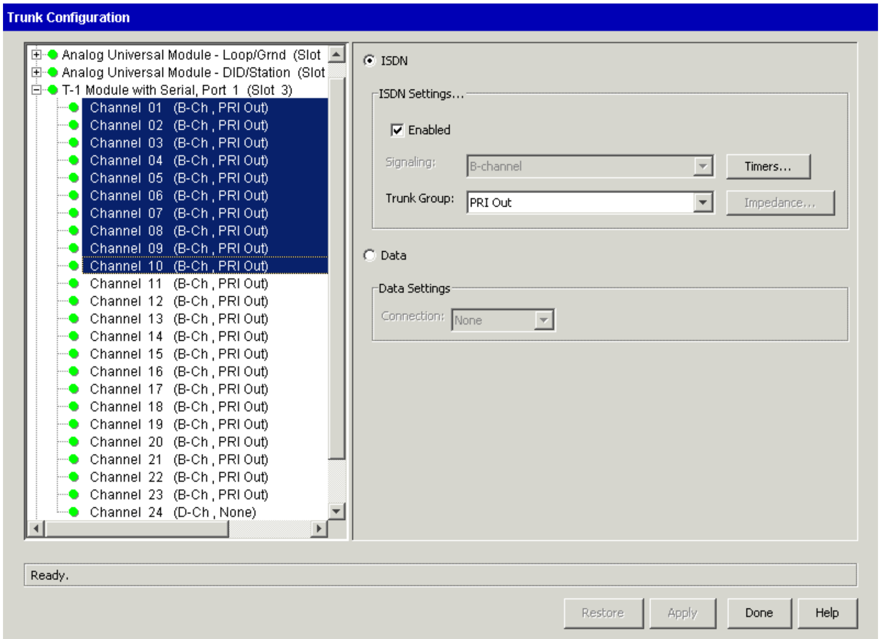
8 Configure the digital channels. (See “Configuring digital channels” on page 5-30.)

9 Click **Apply** to save your changes.

10 Click **Done** to return to the Management Console.

Configuring digital channels

1. Select the card or module according to the steps in “Configuring digital trunk card or module settings” on page 5-23.
2. Display the card or module channels, and select the channels you want to configure.



Trunk Configuration

```
⊞ ● Analog Universal Module - Loop/Grnd (Slot
⊞ ● Analog Universal Module - DID/Station (Slot
⊟ ● T-1 Module with Serial, Port 1 (Slot 3)
    ● Channel 01 (B-Ch , PRI Out)
    ● Channel 02 (B-Ch , PRI Out)
    ● Channel 03 (B-Ch , PRI Out)
    ● Channel 04 (B-Ch , PRI Out)
    ● Channel 05 (B-Ch , PRI Out)
    ● Channel 06 (B-Ch , PRI Out)
    ● Channel 07 (B-Ch , PRI Out)
    ● Channel 08 (B-Ch , PRI Out)
    ● Channel 09 (B-Ch , PRI Out)
    ● Channel 10 (B-Ch , PRI Out)
    ● Channel 11 (B-Ch , PRI Out)
    ● Channel 12 (B-Ch , PRI Out)
    ● Channel 13 (B-Ch , PRI Out)
    ● Channel 14 (B-Ch , PRI Out)
    ● Channel 15 (B-Ch , PRI Out)
    ● Channel 16 (B-Ch , PRI Out)
    ● Channel 17 (B-Ch , PRI Out)
    ● Channel 18 (B-Ch , PRI Out)
    ● Channel 19 (B-Ch , PRI Out)
    ● Channel 20 (B-Ch , PRI Out)
    ● Channel 21 (B-Ch , PRI Out)
    ● Channel 22 (B-Ch , PRI Out)
    ● Channel 23 (B-Ch , PRI Out)
    ● Channel 24 (D-Ch , None)
```

● ISDN

ISDN Settings...

☑ Enabled

Signaling: B-channel

Trunk Group: PRI Out

○ Data

Data Settings

Connection: None

Ready.

Note: If you checked the **ISDN** check box at the digital card or module level in step 4 on page 5-25, you will see channel settings for **ISDN** and **Data** here at the channel level. If you did not check the ISDN check box, you will see channel settings for **Voice** and **Data** here.

3. Select **Voice** or **Data**. Note that if you selected **ISDN** previously, your choices are **ISDN** or **Data**.
4. Configure the appropriate settings based on the channel type.
   - For voice channels, complete “Configuring digital channels for voice” on page 5-31.
   - For data channels, complete “Configuring digital channels for data” on page 5-34.
   - To assign channels to a serial interface, complete “Assigning digital channels to a serial interface” on page 5-36.

Note: For ISDN channels, Channel 24 is automatically set to D-Ch, None.

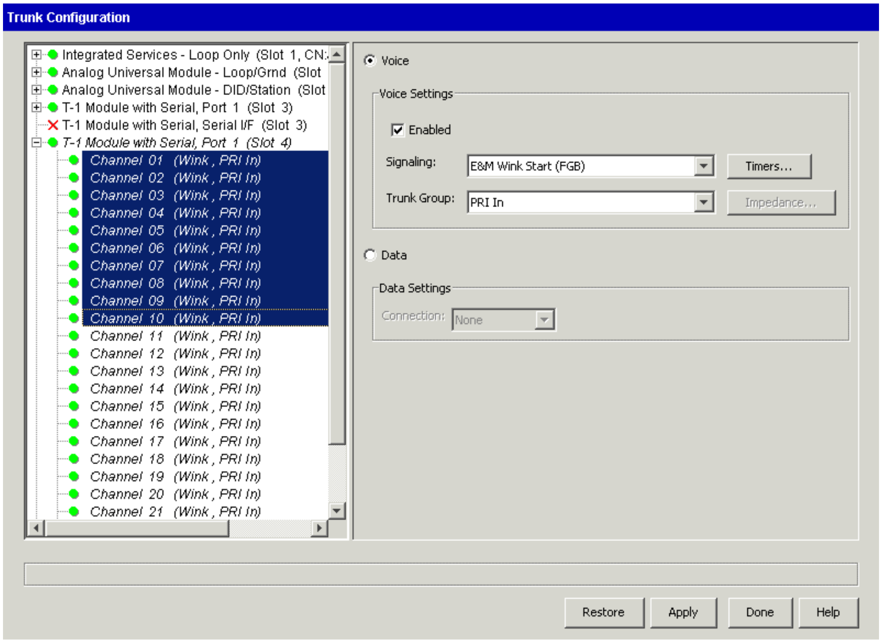
5 Click **Apply** to save your changes.

6 Click **Done** to return to the Management Console.

Configuring digital channels for voice

1 Be sure that the channels are enabled—to do so, select the **Enabled** check box.

2 Select the signaling method from the **Signaling** drop-down list.



Trunk Configuration

- Integrated Services - Loop Only (Slot 1, CN:
- Analog Universal Module - Loop/Grnd (Slot
- Analog Universal Module - DID/Station (Slot
- T-1 Module with Serial, Port 1 (Slot 3)
- T-1 Module with Serial, Serial I/F (Slot 3)
- *T-1 Module with Serial, Port 1 (Slot 4)*
  - *Channel 01 (Wink, PRI In)*
  - *Channel 02 (Wink, PRI In)*
  - *Channel 03 (Wink, PRI In)*
  - *Channel 04 (Wink, PRI In)*
  - *Channel 05 (Wink, PRI In)*
  - *Channel 06 (Wink, PRI In)*
  - *Channel 07 (Wink, PRI In)*
  - *Channel 08 (Wink, PRI In)*
  - *Channel 09 (Wink, PRI In)*
  - *Channel 10 (Wink, PRI In)*
  - *Channel 11 (Wink, PRI In)*
  - *Channel 12 (Wink, PRI In)*
  - *Channel 13 (Wink, PRI In)*
  - *Channel 14 (Wink, PRI In)*
  - *Channel 15 (Wink, PRI In)*
  - *Channel 16 (Wink, PRI In)*
  - *Channel 17 (Wink, PRI In)*
  - *Channel 18 (Wink, PRI In)*
  - *Channel 19 (Wink, PRI In)*
  - *Channel 20 (Wink, PRI In)*
  - *Channel 21 (Wink, PRI In)*

● Voice

Voice Settings

☑ Enabled

Signaling: E&M Wink Start (FGB)

Trunk Group: PRI In

○ Data

Data Settings

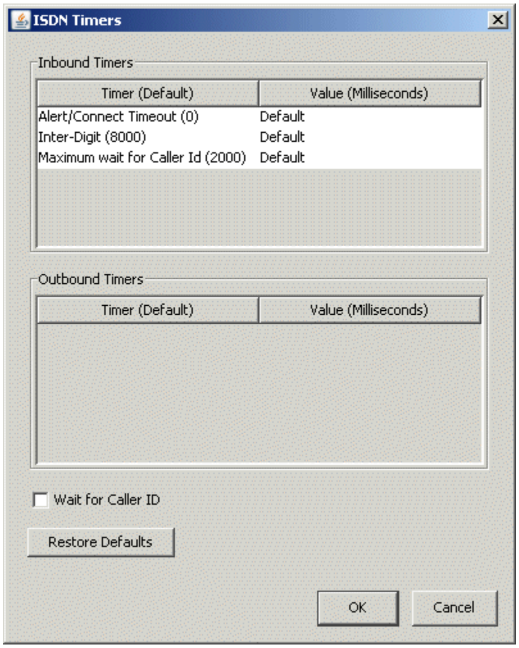
Connection: None

For T-1 voice channels, E&M Wink Start (FGP), E&M Immediate Start, or Ground Start are valid options.

If you have a fractional T-1 trunk, be sure all voice channels that are not in service on your trunk have the **Enabled** check box unchecked.

Note: If you chose the ISDN trunk type when you configured the T-1 module settings, Wave automatically sets the **Signaling** fields for channels 1 through 23 to B-channel; channel 24 is automatically set to D-channel.

3 To enable incoming Caller ID on ISDN trunks, click **Timers**.



Timer (Default)	Value (Milliseconds)
Alert/Connect Timeout (0)	Default
Inter-Digit (8000)	Default
Maximum wait for Caller Id (2000)	Default

□ Wait for Caller ID

In the ISDN Timers dialog, select the **Wait for Caller ID** checkbox.

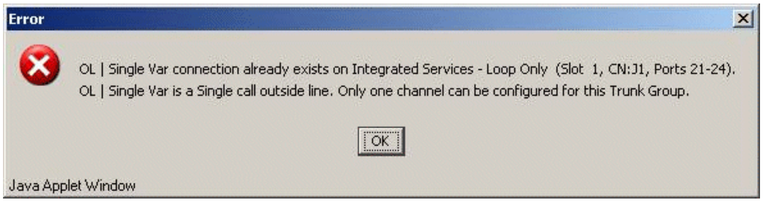
Warning: *Do not change any of the other settings in the ISDN Timers dialog unless you are instructed to do so by your Vertical Technical Support representative in order to address a specific issue.*

4 Click **OK** to close the ISDN Timers dialog.

5 Specify the **Trunk Group** for the selected channels.

One or more channels can be assigned to a particular voice trunk group. For example, if your trunk has 12 (1-12) 2-way voice channels, you can assign the Digital trunk group to channels 1 through 12.

Warning: *If the trunk group you select is a Single Call variant outside line-enabled trunk group and you had previously selected more than one channel in step 2 of "Configuring digital channels" on page 5-30, you will see an error message similar to the following. Click OK to clear the message, and go back and select a single channel:*



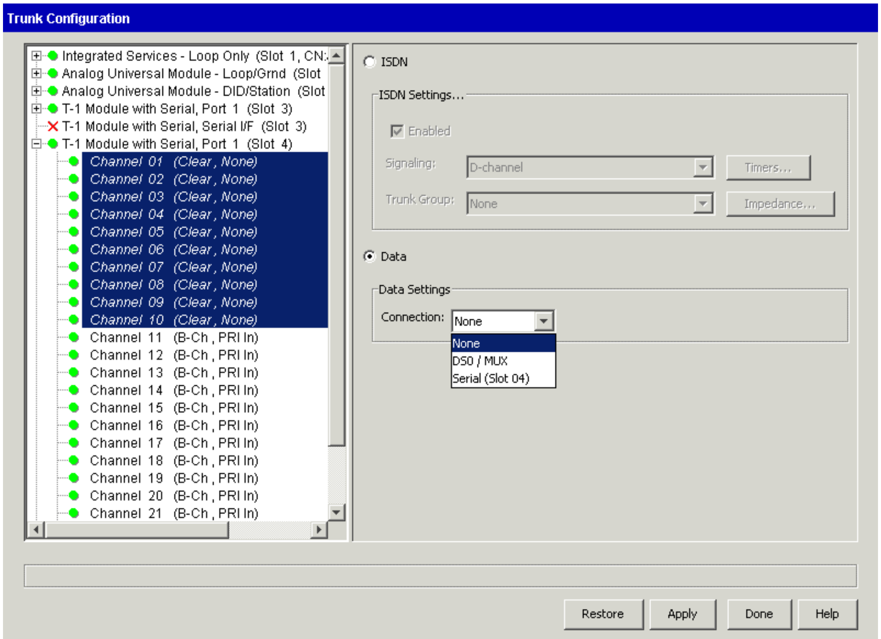
OL | Single Var connection already exists on Integrated Services - Loop Only (Slot 1, CN:J1, Ports 21-24).
OL | Single Var is a Single call outside line. Only one channel can be configured for this Trunk Group.

6 Click **Apply** to save your changes.

7 Click **Done** to return to the Management Console.

Configuring digital channels for data

1 Specify the **Connection** for the selected channels from the drop-down list.


Trunk Configuration
Integrated Services - Loop Only (Slot 1, CN:
Analog Universal Module - Loop/Grnd (Slot
Analog Universal Module - DID/Station (Slot
T-1 Module with Serial, Port 1 (Slot 3)
T-1 Module with Serial, Serial I/F (Slot 3)
T-1 Module with Serial, Port 1 (Slot 4)
Channel 01 (Clear, None)
Channel 02 (Clear, None)
Channel 03 (Clear, None)
Channel 04 (Clear, None)
Channel 05 (Clear, None)
Channel 06 (Clear, None)
Channel 07 (Clear, None)
Channel 08 (Clear, None)
Channel 09 (Clear, None)
Channel 10 (Clear, None)
Channel 11 (B-Ch, PRI In)
Channel 12 (B-Ch, PRI In)
Channel 13 (B-Ch, PRI In)
Channel 14 (B-Ch, PRI In)
Channel 15 (B-Ch, PRI In)
Channel 16 (B-Ch, PRI In)
Channel 17 (B-Ch, PRI In)
Channel 18 (B-Ch, PRI In)
Channel 19 (B-Ch, PRI In)
Channel 20 (B-Ch, PRI In)
Channel 21 (B-Ch, PRI In)
Timers...
Impedance...
None
DS0 / MUX
Serial (Slot 04)
Restore
Apply
Done
Help

○ ISDN

ISDN Settings...

☑ Enabled

Signaling: D-channel

Trunk Group: None

● Data

Data Settings

Connection: None

One or more channels can be assigned to a particular data connection. For example, if your trunk has 12 (13-24) data channels, you can assign the DS0/Mux connection to channels 13 through 24.

Note: Channels assigned to the same digital connection or DS0/Mux trunk group must be contiguous.

You can select from the following connections to transport data between the Wave Server and the WAN:

- **None**
- **DS0/Mux**

  If you are configuring your T-1 trunk to be a T-1/DS0 multiplexor, choose the T-1 DS0/Mux connection for the channels you want to multiplex. You must also assign the same number of channels to T-1DS0/Mux on the other T-1 port.

Note: When a channel is set to T-1/DS0 Mux, the trunk is automatically enabled.

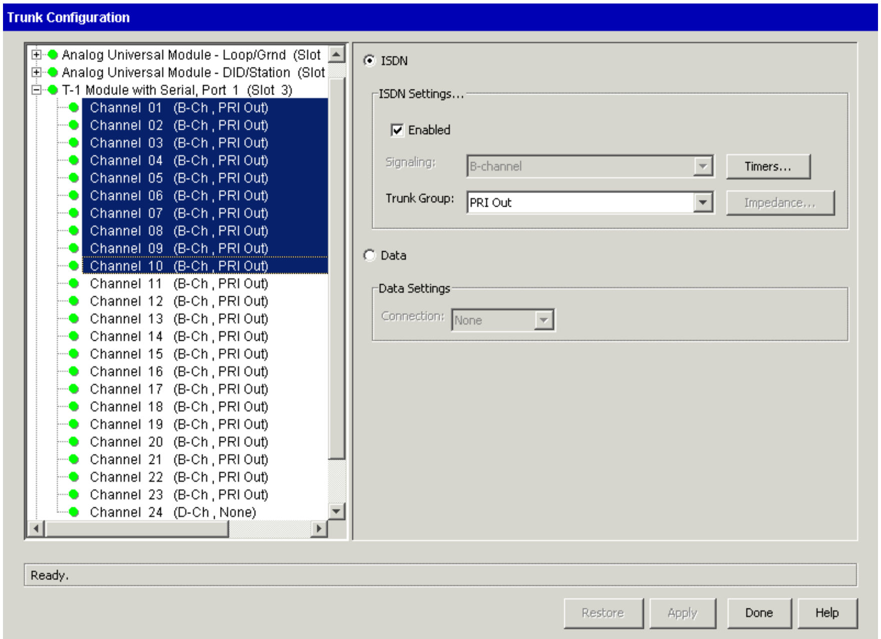
2 Click **Apply** to save your changes.

3 Click **Done** to return to the Management Console.

Configuring digital channels for ISDN

Note: For information about configuring an ISDN data connection for dial-up, see “Configuring dial-up routing” on page 21-1. The information in this section also applies to ISDN PRI.

1 Ensure that the **Enabled** check box is selected.



Trunk Configuration

- Analog Universal Module - Loop/Grnd (Slot
- Analog Universal Module - DID/Station (Slot
- T-1 Module with Serial, Port 1 (Slot 3)
  - Channel 01 (B-Ch , PRI Out)
  - Channel 02 (B-Ch , PRI Out)
  - Channel 03 (B-Ch , PRI Out)
  - Channel 04 (B-Ch , PRI Out)
  - Channel 05 (B-Ch , PRI Out)
  - Channel 06 (B-Ch , PRI Out)
  - Channel 07 (B-Ch , PRI Out)
  - Channel 08 (B-Ch , PRI Out)
  - Channel 09 (B-Ch , PRI Out)
  - Channel 10 (B-Ch , PRI Out)
  - Channel 11 (B-Ch , PRI Out)
  - Channel 12 (B-Ch , PRI Out)
  - Channel 13 (B-Ch , PRI Out)
  - Channel 14 (B-Ch , PRI Out)
  - Channel 15 (B-Ch , PRI Out)
  - Channel 16 (B-Ch , PRI Out)
  - Channel 17 (B-Ch , PRI Out)
  - Channel 18 (B-Ch , PRI Out)
  - Channel 19 (B-Ch , PRI Out)
  - Channel 20 (B-Ch , PRI Out)
  - Channel 21 (B-Ch , PRI Out)
  - Channel 22 (B-Ch , PRI Out)
  - Channel 23 (B-Ch , PRI Out)
  - Channel 24 (D-Ch , None)

● ISDN

ISDN Settings...

☑ Enabled

Signaling: B-channel

Trunk Group: PRI Out

○ Data

Data Settings

Connection: None

Ready.

2 Select a **Trunk Group** from the drop-down list.

3 Click **Apply** to save your changes.

4 Click **Done** to return to the Management Console.

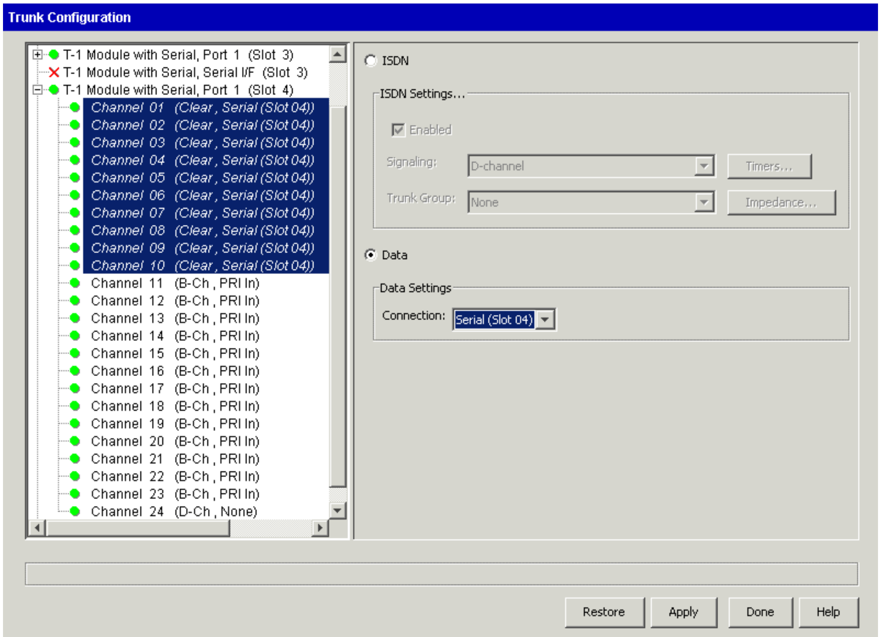
Assigning digital channels to a serial interface

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

1 Select the **Data** option.



Trunk Configuration

- T-1 Module with Serial, Port 1 (Slot 3)
- T-1 Module with Serial, Serial I/F (Slot 3)
- T-1 Module with Serial, Port 1 (Slot 4)
  - *Channel 01 (Clear, Serial (Slot 04))*
  - *Channel 02 (Clear, Serial (Slot 04))*
  - *Channel 03 (Clear, Serial (Slot 04))*
  - *Channel 04 (Clear, Serial (Slot 04))*
  - *Channel 05 (Clear, Serial (Slot 04))*
  - *Channel 06 (Clear, Serial (Slot 04))*
  - *Channel 07 (Clear, Serial (Slot 04))*
  - *Channel 08 (Clear, Serial (Slot 04))*
  - *Channel 09 (Clear, Serial (Slot 04))*
  - *Channel 10 (Clear, Serial (Slot 04))*
  - Channel 11 (B-Ch, PRI In)
  - Channel 12 (B-Ch, PRI In)
  - Channel 13 (B-Ch, PRI In)
  - Channel 14 (B-Ch, PRI In)
  - Channel 15 (B-Ch, PRI In)
  - Channel 16 (B-Ch, PRI In)
  - Channel 17 (B-Ch, PRI In)
  - Channel 18 (B-Ch, PRI In)
  - Channel 19 (B-Ch, PRI In)
  - Channel 20 (B-Ch, PRI In)
  - Channel 21 (B-Ch, PRI In)
  - Channel 22 (B-Ch, PRI In)
  - Channel 23 (B-Ch, PRI In)
  - Channel 24 (D-Ch, None)

○ ISDN

ISDN Settings...

☑ Enabled

Signaling: D-channel

Trunk Group: None

● Data

Data Settings

Connection: Serial (Slot 04)

Hint: Unlike other data channels, you can select and configure *non-contiguous* channels for the serial interface.

2 Select the Serial connection to use from the **Connection** drop-down list.

3 Click **Apply** to save your changes.

4 Click **Done** to return to the Management Console.

Typically, assigning channels to the serial connection is all you need to do. You might want to ensure that your serial interface’s configuration is correct, or make some changes to it, if your connection is not working.

For more information, see “Ensuring that the T-1 serial interface is set correctly” on page 14-1.

Configuring ports and channels on the Quad BRI Module

The Quad BRI Module supports ISDN Basic Rate Interface (BRI) digital trunks. The Quad BRI Module provides connectivity between the Wave Server and Central Office (CO) equipment supporting Euro-ISDN BRI communication protocols.

The Quad BRI Module supports 4 Euro-ISDN BRI trunks and up to 8 simultaneous voice calls.

Note: The following procedures call out information specific to configuring ports and channels on the Quad BRI Module. For more about general trunk and channel configuration settings not described in detail here, see "Configuring digital trunks and channels" on page 5-22. Also, refer to your Service Confirmation Letter or contract to determine specific settings to use.

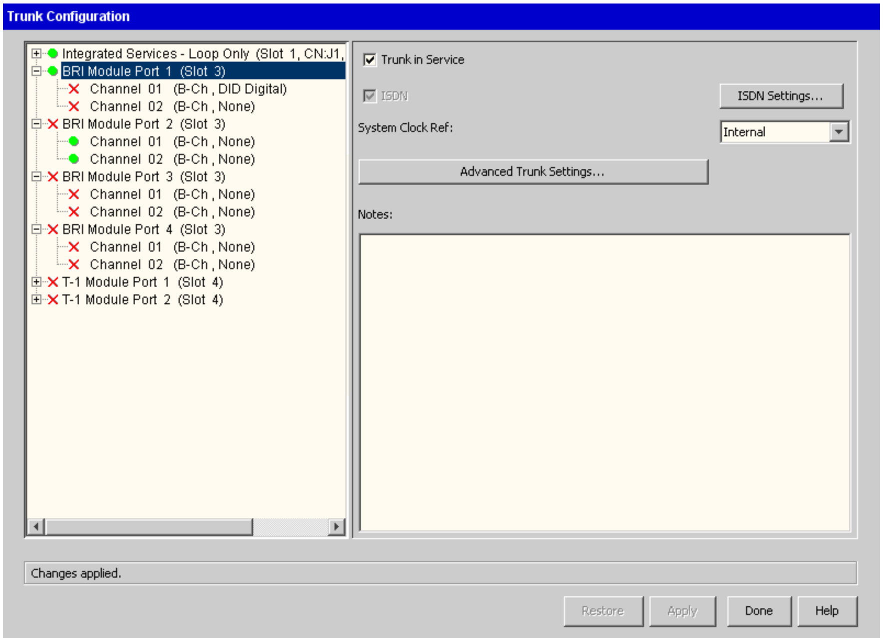
To configure ports on the Quad BRI Module

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

1 In the Trunk Configuration applet, select the port, and then select the **Trunk in Service** checkbox.



Trunk Configuration

- ● Integrated Services - Loop Only (Slot 1, CN:J1,
- ● BRI Module Port 1 (Slot 3)
  - ✕ Channel 01 (B-Ch , DID Digital)
  - ✕ Channel 02 (B-Ch , None)
- ✕ BRI Module Port 2 (Slot 3)
  - ● Channel 01 (B-Ch , None)
  - ● Channel 02 (B-Ch , None)
- ✕ BRI Module Port 3 (Slot 3)
  - ✕ Channel 01 (B-Ch , None)
  - ✕ Channel 02 (B-Ch , None)
- ✕ BRI Module Port 4 (Slot 3)
  - ✕ Channel 01 (B-Ch , None)
  - ✕ Channel 02 (B-Ch , None)
- ✕ T-1 Module Port 1 (Slot 4)
- ✕ T-1 Module Port 2 (Slot 4)

☑ Trunk in Service

☑ ISDN

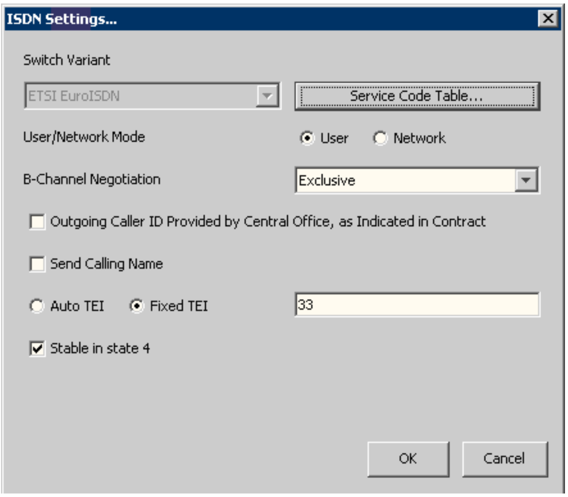
System Clock Ref: Internal

Notes:

Changes applied.

Note: The **ISDN** checkbox is always selected for each port on the Quad BRI module, and cannot be changed. Also, the **Advanced Settings** button is disabled.

2 Click the **ISDN settings** button. The ISDN Settings dialog opens.



ISDN Settings...

Switch Variant: ETSI EuroISDN

User/Network Mode ● User ○ Network

B-Channel Negotiation: Exclusive

□ Outgoing Caller ID Provided by Central Office, as Indicated in Contract

□ Send Calling Name

○ Auto TEI ● Fixed TEI 33

☑ Stable in state 4

Note: The Switch Variant ‘ETSI EuroISDN’ is automatically selected and cannot be changed. You do not need to modify the Service Code Table during initial configuration—the defaults should be sufficient for connecting to a local exchange carrier.

3 Enter the following information:

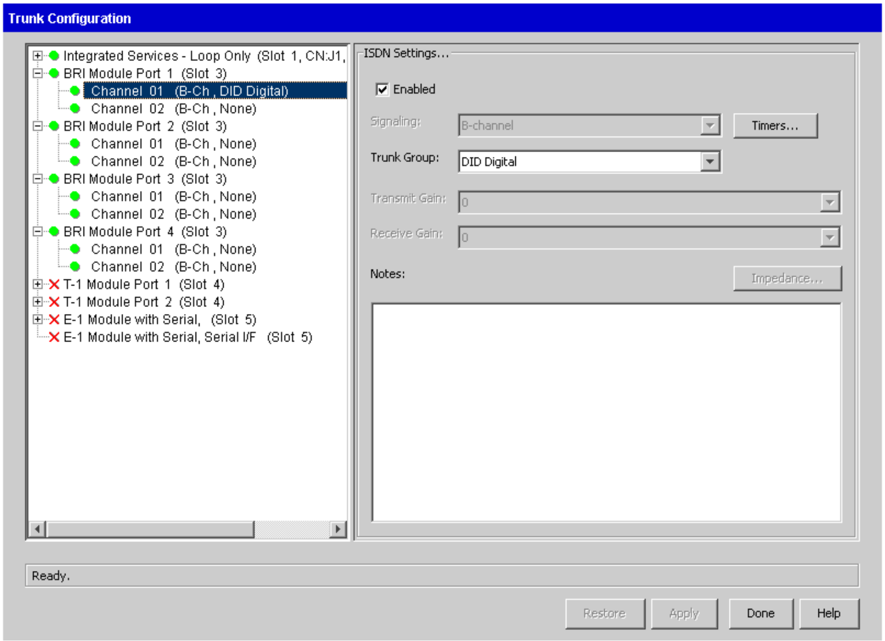
- **User/Network Mode**. Select one of the following:
  - Select **User** (the default) if you are configuring this port or ports to communicate over an external BRI trunk to the CO.
  - Select **Network** if you are configuring this port or ports to communicate over an internal BRI trunk to an ISDN device such as a fax machine, modem, and so forth.
- **B Channel Negotiation**. Select **Exclusive** or **Preferred** from the drop-down list.
- **Send Calling Name**. Select this checkbox if you want Wave to send the name specified in the General Settings applet when calls are sent over this trunk.
- Specify the TEI (Terminal Endpoint Identifier) to use. TEI is a code supplied by an ISDN device and is used by the service provider switch to identify the calling device. Select one of the following:
  - **Auto TEI**. Auto TEI is obtained from the network via a message protocol, and is typically used for point-to-multipoint configurations.
  - **Fixed TEI**. Enter a value between 0-63 inclusive in the text box. Typically, a TEI value of 0 is used in a point to point configuration.
- **Stable in state 4**. *This option is not supported in this version.*

4 Click **OK** to save your changes.

5 Repeat these steps for the other ports on the Quad BRI module.

To configure channels on the Quad BRI Module

1 In the Trunk Configuration applet, select the channel or channels on the Quad BRI Module that you want to configure, and then select the **Enabled** checkbox.



Trunk Configuration

- Integrated Services - Loop Only (Slot 1, CN:J1,
- BRI Module Port 1 (Slot 3)
  - Channel 01 (B-Ch , DID Digital)
  - Channel 02 (B-Ch , None)
- BRI Module Port 2 (Slot 3)
  - Channel 01 (B-Ch , None)
  - Channel 02 (B-Ch , None)
- BRI Module Port 3 (Slot 3)
  - Channel 01 (B-Ch , None)
  - Channel 02 (B-Ch , None)
- BRI Module Port 4 (Slot 3)
  - Channel 01 (B-Ch , None)
  - Channel 02 (B-Ch , None)
- ✕ T-1 Module Port 1 (Slot 4)
- ✕ T-1 Module Port 2 (Slot 4)
- ✕ E-1 Module with Serial, (Slot 5)
- ✕ E-1 Module with Serial, Serial I/F (Slot 5)

ISDN Settings...

☑ Enabled

Signaling: B-channel

Trunk Group: DID Digital

Transmit Gain: 0

Receive Gain: 0

Notes:

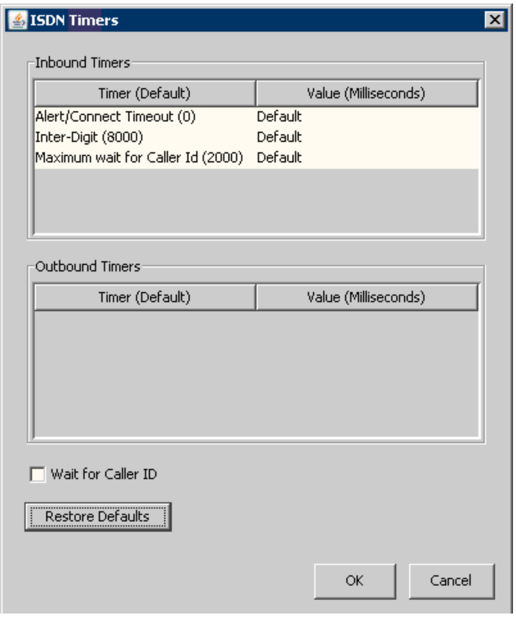
Ready.

Note: The **Signaling** setting defaults to B-channel and cannot be changed. The **Transmit Gain** and **Receive Gain** settings do not apply to the Quad BRI Module and are disabled, as well as the **Impedance** button.

2 Select the **Trunk Group** for the selected channels from the drop-down list.

3 Enter any additional **Notes** for reference.

4 To enable incoming Caller ID on BRI trunks, click the **Timers** button. The ISDN Timers dialog opens.



ISDN Timers

Inbound Timers

Timer (Default)	Value (Milliseconds)
Alert/Connect Timeout (0)	Default
Inter-Digit (8000)	Default
Maximum wait for Caller Id (2000)	Default

Outbound Timers

Timer (Default)	Value (Milliseconds)

□ Wait for Caller ID

5 Select the **Wait for Caller ID** checkbox.

Note: Do not change any of the other settings in the ISDN Timers dialog unless you are instructed to do so by your Vertical Technical Support representative in order to address a specific issue.

6 Click **OK** to save your changes.

7 Repeat these steps for the other ports on the Quad BRI module.

Enabling trunks for external pager and call notifications

For any trunks that will be used for external pager or call notifications, you must make the following configuration changes in order for these features to work. This information applies to all trunk types.

Note: For information on how to set up notifications for a user, see “The Voice Mail \ E-mail, Pager, and Call Notification tabs” on page 11-42.

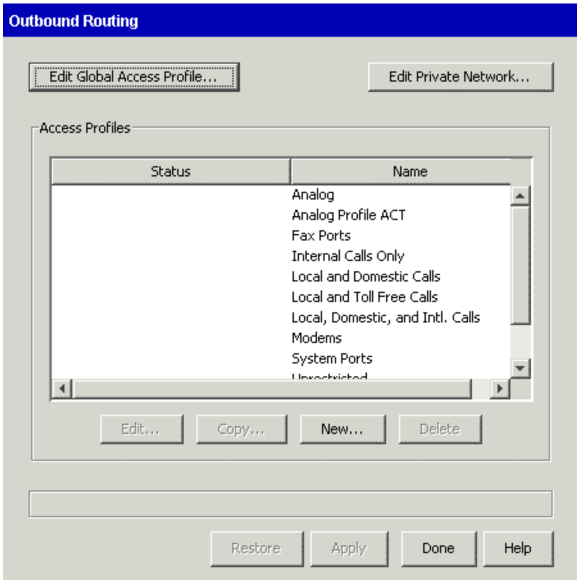
To enable trunks for external pager and call notifications

1 If necessary, click the Administration tab of the Management Console.

Click

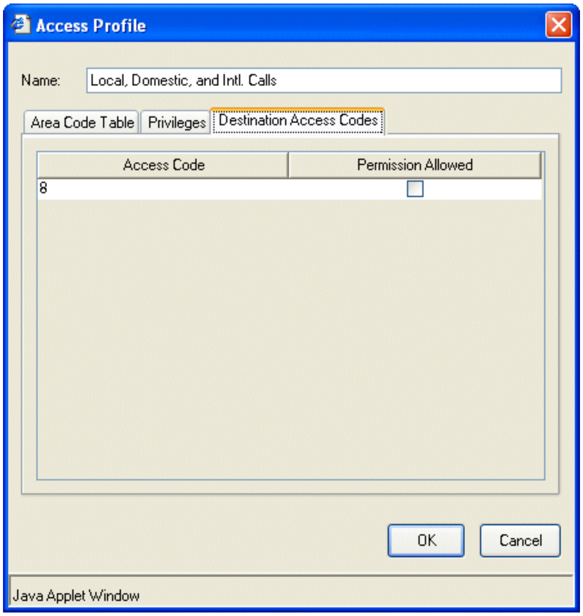
2 Click the Outbound Routing icon, located in the Trunk Administration section.

3 The Outbound Routing dialog opens.



Status	Name
	Analog
	Analog Profile ACT
	Fax Ports
	Internal Calls Only
	Local and Domestic Calls
	Local and Toll Free Calls
	Local, Domestic, and Intl. Calls
	Modems
	System Ports
	Unrestricted

4 Select the **System Ports** access profile and click **Edit**. When the Access Profile dialog box opens, click the Destination Access codes tab.



Name: Local, Domestic, and Intl. Calls

Access Code	Permission Allowed
8	□

5 Select the **Permission Allowed** checkbox for all access codes that are being used for external pager and call notifications. In the example above, “8” was set up previously as a trunk access code in the First Digit Table. (See “About the First Digit Table” on page 7-1.)

6 Click **OK**, and then click **Done**.

Chapter 6

IP Telephony Configuration

Chapter Contents

This chapter describes how to configure the IP telephony features available on the Wave Server.

Allocating IP telephony resources

Before you configure your system for IP telephony, you must allocate Digital Signaling Processor (DSP) resources that are required for each IP telephony port. For more information about the DSP resources required for IP telephony, refer to DSP resources and licensing for IP telephony resources. Note the following:

- You must have a SIP Trunk license added on the Wave Server before you can configure SIP trunks. See Chapter 24 for instructions.
- Additional Voice Over IP DSP resources are used only briefly during the life a of a call or while a feature is being used—in this version, you must allocate these resources manually. See “Resource requirements for transitory events” on page 23-44.

To allocate IP telephony resources

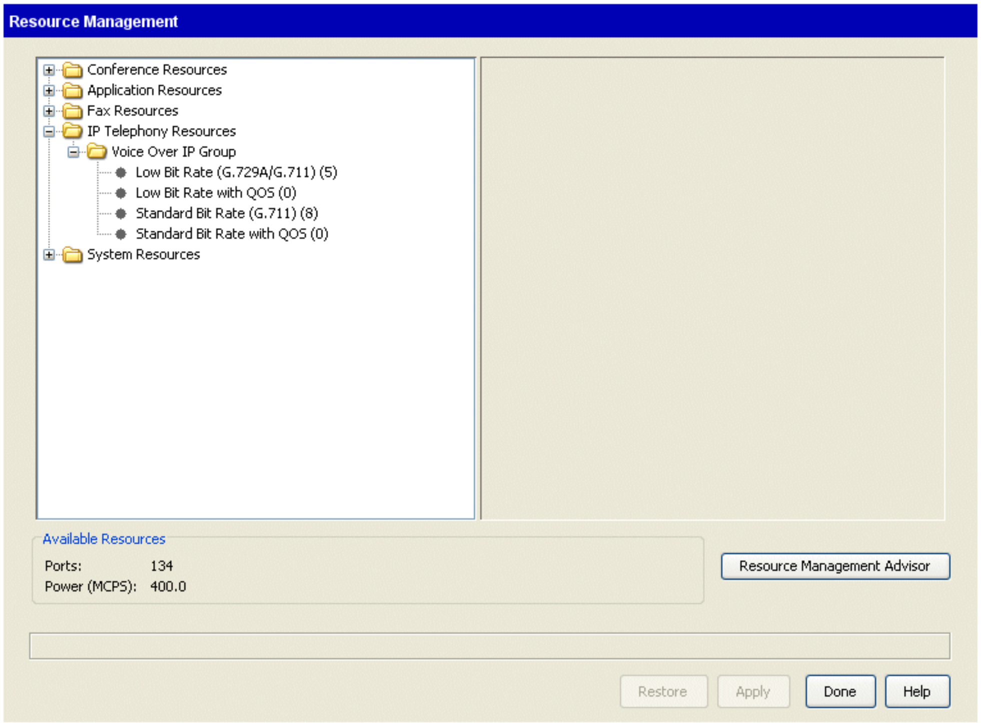
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Resource Management icon, located in the PBX Administration section

3 Expand the IP Telephony Resources folder.

4 Expand the Voice Over IP Group folder, and select the **G.729A/G.711** codec.



5 Select the appropriate number of available IP telephony resources in the drop-down list (on the right side of the applet).

6 Click **Apply** to save your changes, and return to the Management Console.

Configuring site-to-site call routing for IP telephony

You configure call routing in order to use Signaling Control Points for the following outbound call routing scenarios:

- **Automatic route selection**. See “Automatic route selection” on page 29-8.
- **Off-premise extensions**. See “Off-premise extensions” on page 29-13.
- **Destination access codes**. See “Destination access code/direct to trunk group” on page 29-14.

See Chapter 9 for information about configuring outbound call routing.

To configure call routing for IP call destinations you will need to perform the following procedures:

- Enabling IP telephony or SIP signaling protocols. See page 6-4.
- Setting up SIP endpoint authentication. See page 6-10.
- Configuring Signaling Control Points. See page 6-14.
- Configuring default inbound IP call routing. See page 6-26.
- Including Signaling Control Points in the outbound call routing configuration. See page 6-28.

Enabling IP telephony or SIP signaling protocols

Perform the following steps to enable the SIP signaling protocol on the Wave Server. Note that you need to do so to use SIP phones with Wave, even if you are not using SIP trunks.

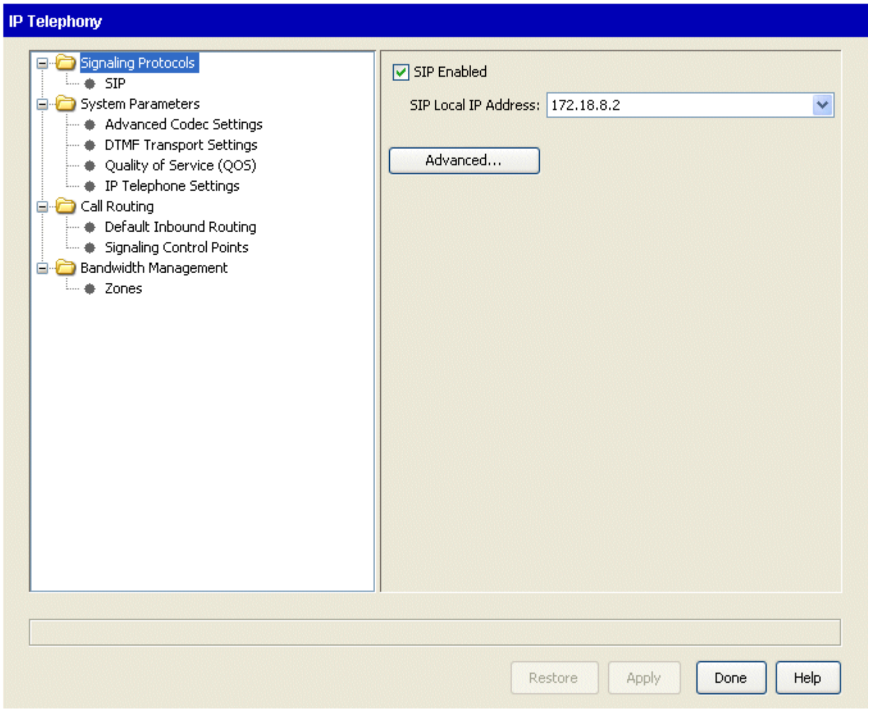
To enable IP telephony or SIP signaling protocols

1 If necessary, click the Administration tab of the Management Console.

Click IP

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Click **SIP** from the Signaling Protocols folder in the left pane.



IP Telephony

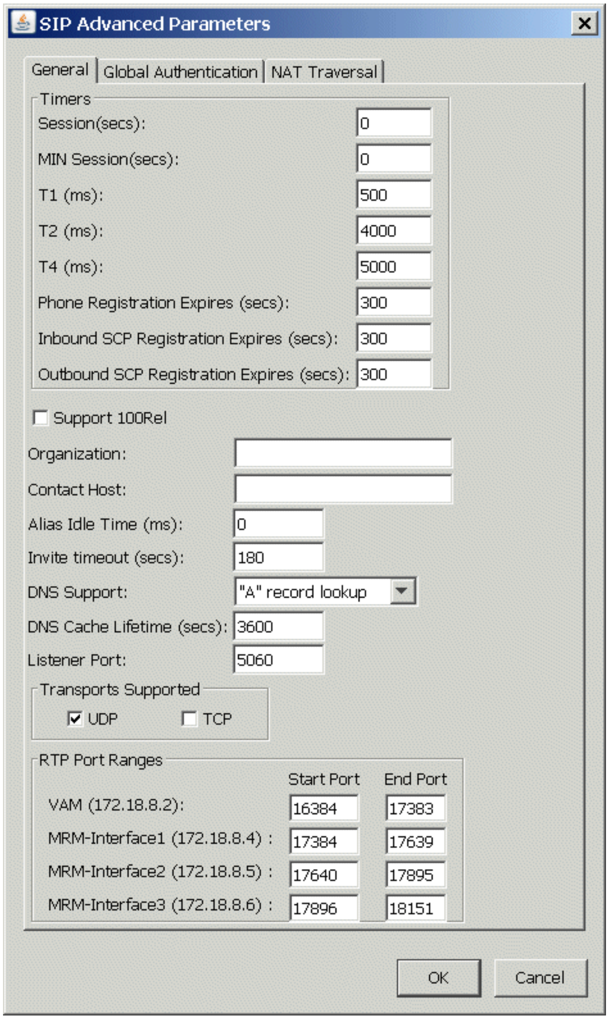
- Signaling Protocols
  - SIP
- System Parameters
  - Advanced Codec Settings
  - DTMF Transport Settings
  - Quality of Service (QOS)
  - IP Telephone Settings
- Call Routing
  - Default Inbound Routing
  - Signaling Control Points
- Bandwidth Management
  - Zones

☑ SIP Enabled

SIP Local IP Address: 172.18.8.2

4 Select the **SIP Enabled** checkbox. The **SIP Local IP Address** is selected by default.

Clicking **Advanced** opens the SIP Advanced Parameters dialog.



SIP Advanced Parameters

Timers

Session(secs):	0
MIN Session(secs):	0
T1 (ms):	500
T2 (ms):	4000
T4 (ms):	5000
Phone Registration Expires (secs):	300
Inbound SCP Registration Expires (secs):	300
Outbound SCP Registration Expires (secs):	300

□ Support 100Rel

Organization:	
Contact Host:	
Alias Idle Time (ms):	0
Invite timeout (secs):	180
DNS Support:	"A" record lookup
DNS Cache Lifetime (secs):	3600
Listener Port:	5060

Transports Supported

☑ UDP □ TCP

RTP Port Ranges

	Start Port	End Port
VAM (172.18.8.2):	16384	17383
MRM-Interface1 (172.18.8.4) :	17384	17639
MRM-Interface2 (172.18.8.5) :	17640	17895
MRM-Interface3 (172.18.8.6) :	17896	18151

- **Global Authentication tab**. Use this tab to set up SIP authentication, as described in “Setting up SIP endpoint authentication” on page 6-10.
- **General tab**. Use this tab to adjust advanced SIP timers.

Modifying advanced SIP timers

Important! These are expert settings that should not be modified unless you are directed to do so by your Vertical Technical Support representative. Applying changes that you make to any of the SIP timers on this tab will cause all current SIP calls to be dropped, so be sure to make changes at an appropriate time.

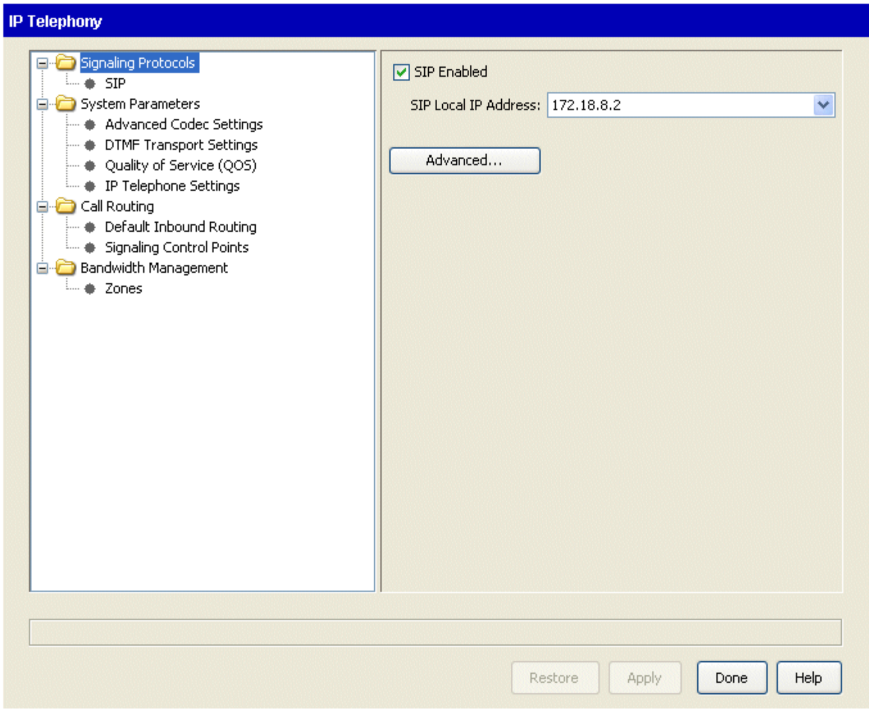
To modify advanced SIP timers

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

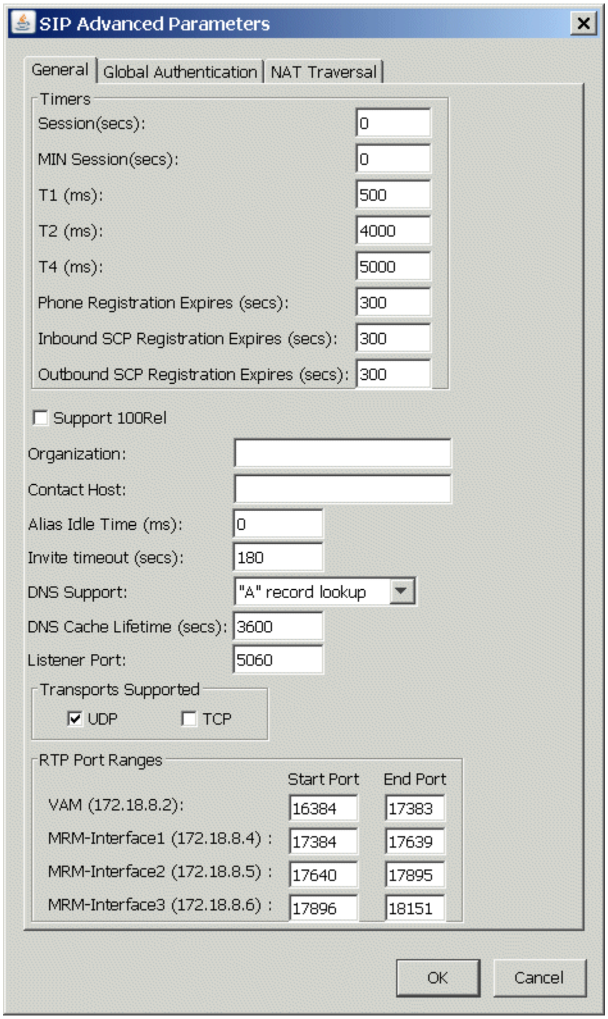
3 Expand the Signaling Protocols folder in the left pane if necessary, and then click **SIP**.



☑ SIP Enabled

SIP Local IP Address: 172.18.8.2

4 Click **Advanced** to open the SIP Advanced Parameters dialog. Click the General tab.



SIP Advanced Parameters

Timers

Session(secs):	0
MIN Session(secs):	0
T1 (ms):	500
T2 (ms):	4000
T4 (ms):	5000
Phone Registration Expires (secs):	300
Inbound SCP Registration Expires (secs):	300
Outbound SCP Registration Expires (secs):	300

□ Support 100Rel

Organization:	
Contact Host:	
Alias Idle Time (ms):	0
Invite timeout (secs):	180
DNS Support:	"A" record lookup
DNS Cache Lifetime (secs):	3600
Listener Port:	5060

Transports Supported

☑ UDP □ TCP

RTP Port Ranges

	Start Port	End Port
VAM (172.18.8.2):	16384	17383
MRM-Interface1 (172.18.8.4) :	17384	17639
MRM-Interface2 (172.18.8.5) :	17640	17895
MRM-Interface3 (172.18.8.6) :	17896	18151

5 Make your changes:

- The following SIP Session timers can be used to define keep-alive values for SIP sessions. In Wave, a Session is a SIP call. On long calls, if an endpoint drops off due to a network issue, Wave may think the call is still in progress even though both parties have hung up.

The default values balance how long you are willing to allow a missing call to go detected without creating too much unnecessary network traffic. You should not modify the default values unless you have identified a specific problem and are instructed to do so by your Wave technical support representative.

- **Session (secs)**. Specifies the length of time in seconds after which the endpoint must send a periodic re-INVITE or UPDATE message to Wave.
- **MIN Session (secs)**. Specifies the minimum value Wave will accept from an endpoint for a periodic message to Wave.

- **T1 (ms)**. Specifies the duration (in milliseconds) before the first retransmission of a request over UDP, or an INVITE response over any transport protocol. Subsequent retransmission intervals are calculated by doubling this initial value, up to a maximum value configured in the T2 Timer value. The minimum recommended value is 500ms. Your Vertical Technical Support representative may increase the value of this timer if you are communicating with SIP end points over network connections with longer latencies.
- **T2 (ms)**. Specifies the maximum duration (in milliseconds) before a request is retransmitted over UDP or an INVITE response is retransmitted over any transport protocol. It must be greater than or equal to the value configured in the T1 Timer. The minimum recommended value is 4000ms.
- **T4 (ms)**. Specifies the maximum lifetime of a transaction in the SIP network. After a transaction completes, it is the amount of time that a UAS will retain the transaction information in order to subsume late duplicate responses.
- The following SIP registration expiration timers control the length of time in seconds before a SIP phone or SCP attempts to reregister. Each expiration timer defines a “quiet time” during which the the SIP endpoint (SIP phone or SCP) does not need to be exchanging data with Wave to still be considered “In Service”. An endpoint that goes out of service during the quiet time will not be detected until it fails to complete a registration when the timer expires. Shortening an expiration timer will allow Wave to detect an out-of-service condition sooner, but will increase network traffic.

  The default values balance keeping the endpoint status up to date without creating too much unnecessary network traffic. You should not modify the default values unless you have identified a specific issue with a unique ITSP or third-party phone.

  - **Phone Registration Expires (secs)**. Specifies the minimum time in seconds within which the phone must send a periodic registration packet to Wave in order for Wave to keep the phone in the “In Service” state. If this timer expires for a particular phone, the phone will be considered “Out of Service”.

- **Inbound SCP Registration Expires (secs)**. Specifies the minimum time in seconds within which the SCP must send a periodic registration packet to Wave in order for Wave to keep the SCP in the “In Service” state. If this timer expires, the SCP will be considered “Out of Service”.
- **Outbound SCP Registration Expires (sec)**. Specifies the minimum time in seconds within which Wave must send a periodic registration packet to the SCP. The SCP may respond to a registration packet with a different timer value, in which case Wave will use the smaller of the two values. If the SCP fails to respond to a registration packet, Wave will place the SCP in the “Out of Service” state and continue to send periodic registration packets to the SCP. If the SCP sends a positive response to a registration packet, Wave will place the SCP in the “In Service” state.

6 Click **Apply** to save your changes.

Setting up SIP endpoint authentication

Wave supports authentication of inbound requests for SIP endpoints. A SIP endpoint can be either a SIP extension or a SIP Signaling Control Point (SCP). When properly configured, Wave can serve as user agent client (UAC), user agent server (UAS), or a back-to-back user agent (B2BUA) under different call scenarios:

- When Wave serves as a UAS or a B2BUA, Wave authenticates and authorizes incoming requests from clients registering to it or wishing to route calls through it.
- When Wave serves as a UAC, it provides appropriate authentication credentials when challenged by the remote UAS.

Specifically, Wave performs the following SIP endpoint authentication functions:

- Authentication of incoming registrations from SIP phones configured as extensions on Wave.
- Authentication of incoming calls from SIP phones configured as extensions on Wave.
- Authentication of outbound registrations for SCPs that are challenged by the remote UAS.
- Authentication of outbound calls through SCPs that are challenged by the remote UAS.

In very simple terms, registration is the process of assigning an address to a SIP extension or SIP SCP, and authentication is the process of verifying the identity of the SIP extension or SIP SCP before updating the address in the Wave data base.

You set up SIP endpoint authentication parameters in the several places:

- **To set up global SIP endpoint authentication parameters that are used unless a specific SCP has its own authentication parameters**, you use the IP Telephony applet, SIP Advanced Parameters dialog (Global Authentication tab). See “Setting up global SIP endpoint authentication parameters” on page 6-11.
- **To to set up SIP endpoint authentication parameters for a specific SCP**, you use the IP Telephony applet, Signaling Control Point dialog (SIP Settings tab). See “Configuring Signaling Control Points” on page 6-14.
- **To specify a user’s SIP endpoint authentication password**, you use the User/Group Management applet, User dialog (Phone tab). See “The Phone \ SIP tab” on page 11-79.

Setting up global SIP endpoint authentication parameters

Perform the following steps starting on to set up global SIP endpoint authentication parameters that are used unless a specific SCP has its own authentication parameters.

Global SIP endpoint authentication best practice

Starting with Wave 4.0, global SIP endpoint authentication will be enabled by default on all new Wave Servers—this will enforce that all SCPs use a password to authenticate unless this option is purposely turned off. (Previously, global SIP authentication was disabled by default.)

Important! This change will *not* be applied to existing Wave Servers that are upgraded to Wave 4.0 or higher. ***Vertical strongly recommends that global SIP endpoint authentication be enabled on all existing Wave Servers as a standard security measure.*** You do so in the SCP Settings section in the SIP Advanced Settings dialog, as described below.

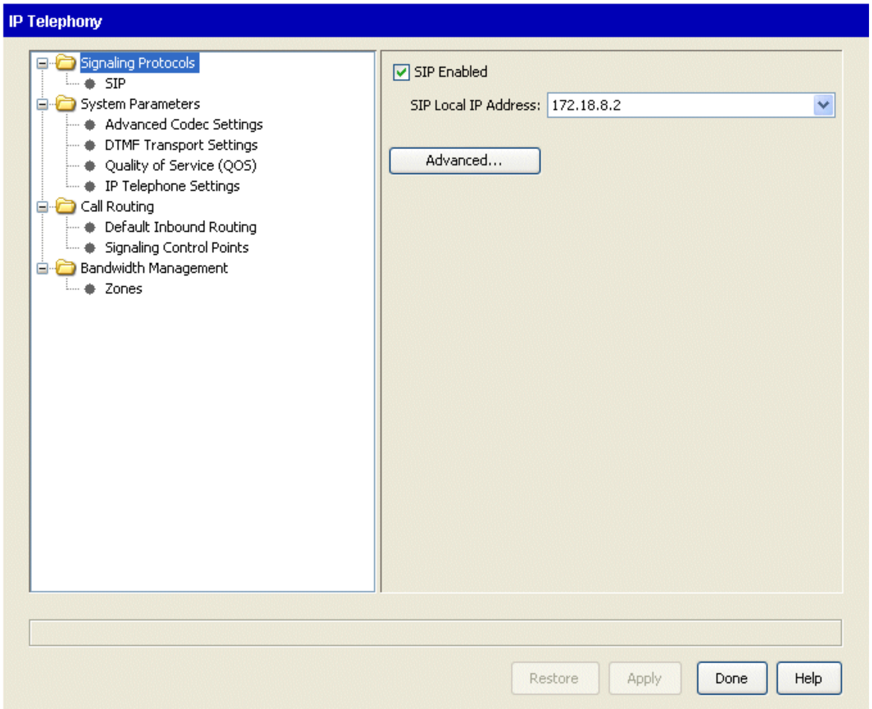
To set up global SIP endpoint authentication parameters

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Expand the Signaling Protocols folder in the left pane if necessary, and then click **SIP**.



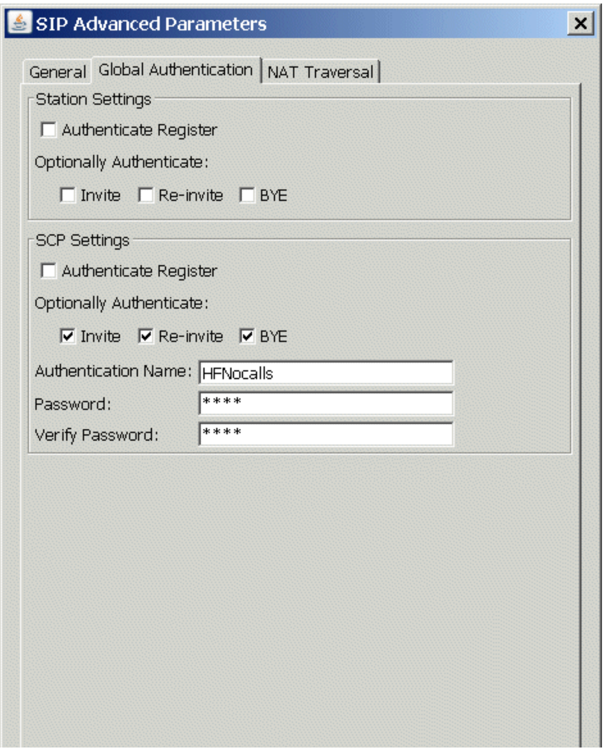
IP Telephony

- Signaling Protocols
  - SIP
- System Parameters
  - Advanced Codec Settings
  - DTMF Transport Settings
  - Quality of Service (QOS)
  - IP Telephone Settings
- Call Routing
  - Default Inbound Routing
  - Signaling Control Points
- Bandwidth Management
  - Zones

☑ SIP Enabled

SIP Local IP Address: 172.18.8.2

4 Click **Advanced** to open the SIP Advanced Parameters dialog. Click the Global Authentication tab.



SIP Advanced Parameters

Station Settings

□ Authenticate Register

Optionally Authenticate:

□ Invite □ Re-invite □ BYE

SCP Settings

□ Authenticate Register

Optionally Authenticate:

☑ Invite ☑ Re-invite ☑ BYE

Authentication Name: HFNocalls

Password: ****

Verify Password: ****

5 Enter the following information in the Station Settings section, based on the level of authentication you require. See your Vertical support representative for more information about how to use these settings.

- **Authenticate Register**
- **Optionally Authenticate**:
  - **Invite**.
  - **Re-Invite**
  - **BYE**

6 Enter the following information in the SCP Settings section, based on the level of authentication you require. See your Vertical support representative for more information about how to use these settings.

- **Authenticate Register**. Starting in Wave 4.0, this option is selected by default on all *new* Wave Servers. ***Vertical strongly recommends that global SIP endpoint authentication be enabled on all Wave Servers as a standard security measure.***
- **Optionally Authenticate**:
  - **Invite**
  - **Re-Invite**
  - **BYE**

7 For the following fields, enter the authentication credentials provided by the remote SIP endpoint administrator. These three fields are disabled until you select any of the checkboxes in the previous step. These fields are required when they are enabled.

Note: Starting in Wave 4.0, the default **Authentication Name** and **Password** on all *new* Wave Servers is “TemporaryAuthName” and “TemporaryAuthPassword”.

- **Authentication Name**. 1-32 alphanumeric characters. Authentication name cannot match an existing extension plus last name (for example, “Ryan605”) or another SCP's authentication name.
- **Password**. 1-48 characters.
- **Verify Password**.

8 Click **Apply** to save your changes.

Configuring Signaling Control Points

You configure a Signaling Control Point (SCP) to determine how to handle IP calls to and from a specific IP address that represents a SIP destination endpoint. The following steps also describe how to configure SIP endpoint authentication settings specific to this SCP.

You can adjust the amount of time that a Signaling Control Point step in an outbound routing table is given to operate before the system tries the next step in the table. See “Setting the route step timeout” on page 6-25.

To configure a Signaling Control Point

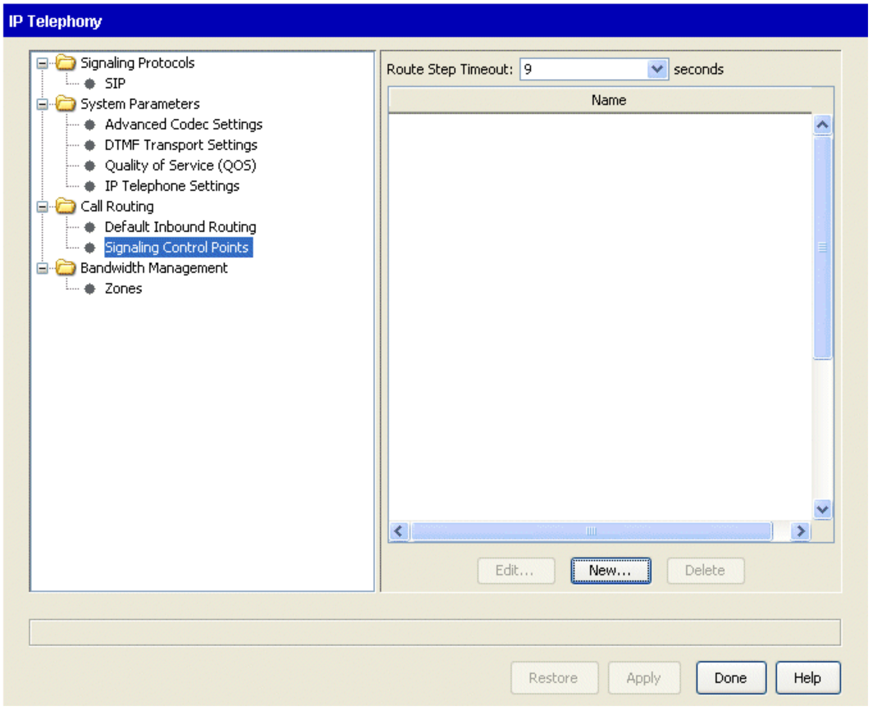
Click

IP

1 If necessary, click the Administration tab of the Management Console.

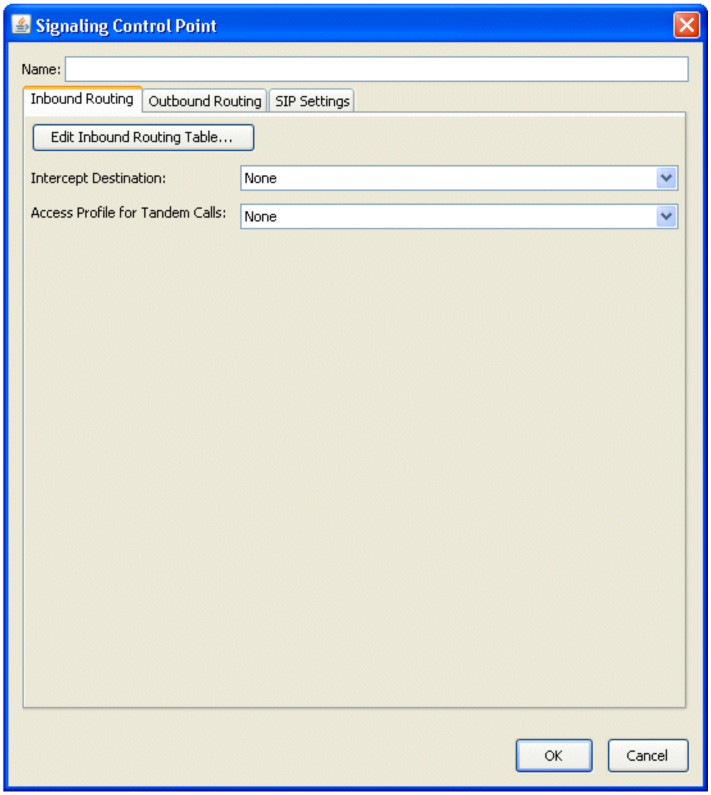
2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select **Signaling Control Points** from the Call Routing folder in the left pane.



Route Step Timeout: 9 seconds

4 Click **New** to add a new SCP, or select an existing SCP to edit, then click **Edit**. The Signaling Control Point dialog opens.



Intercept Destination: None

Access Profile for Tandem Calls: None

5 Enter a **Name** for the SCP.

When you configure outbound call routing, this name will appear as IP, a vertical bar (|), and the name you enter here. For example, if you enter New York, it will be displayed as IP|New York in your outbound call routing configuration. See “Including Signaling Control Points in the outbound call routing configuration” on page 6-28 for more information.

Note: The **Name** field accepts alphanumeric characters as well as the following special characters: `` ` ~ ! # $ % & * ( ) - = + | { } ; : " , . / < > ? ``

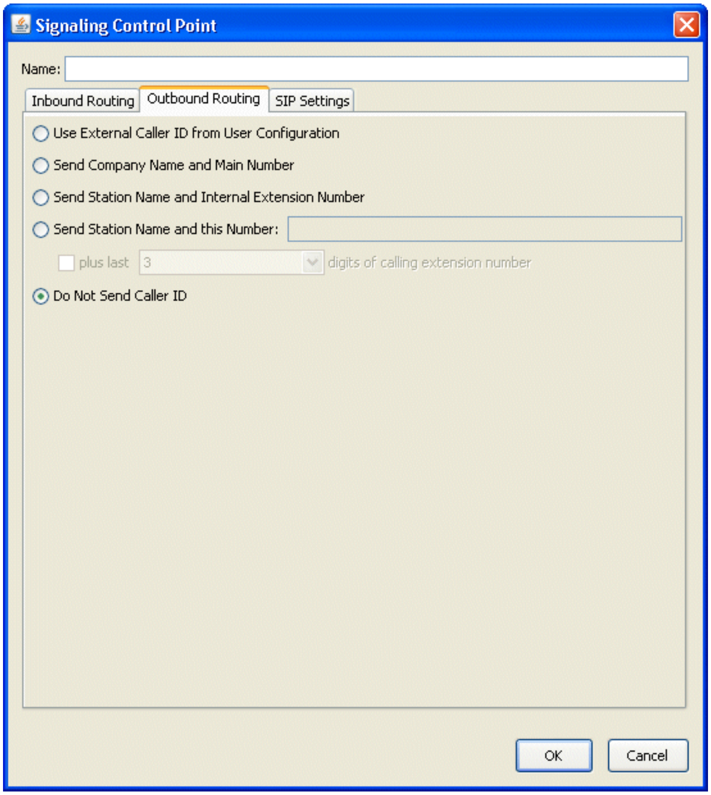
6 On the Inbound Routing tab, configure the settings for handling calls received from this SCP.

- **Intercept Destination**. Select the extension to which calls from this SCP that cannot be matched in the Inbound Routing table will be routed.
- **Access Profile for Tandem Calls**. Select the access profile to apply to calls received from this SCP that will be connecting to another trunk. (Access profiles identify the different calling privileges that can be associated with extensions, trunk groups, digital connections, and SCPs. See “Configuring specific access profiles” on page 9-14 for more information.)

  Warning! *If you have not modified the default “Unrestricted” access profile, be aware that selecting that access profile here could leave your system vulnerable to hackers who are able to identify your Tandem Access Profile number.*

7 Click **Edit Inbound Routing Table** to specify the call sources, schedules, and routing. For more information, see “Configuring inbound routing tables” on page 8-4.

8 On the Outbound Routing tab, choose one of the Caller ID formats for sending Caller ID with calls to this SCP. (For more about Caller ID, see “Configuring Caller ID” on page 16-6.))



Signaling Control Point

Name:

○ Use External Caller ID from User Configuration

○ Send Company Name and Main Number

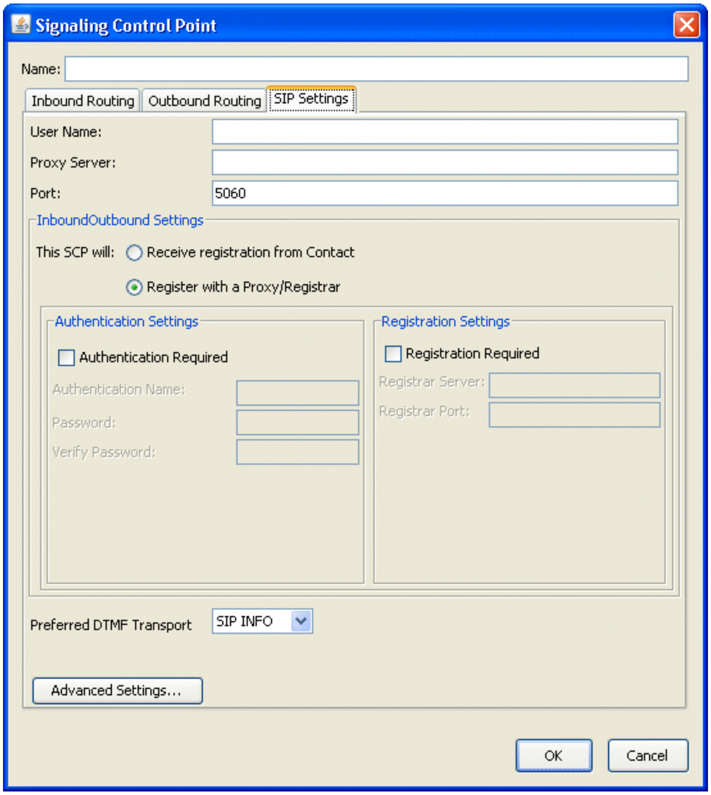
○ Send Station Name and Internal Extension Number

○ Send Station Name and this Number:

□ plus last 3 digits of calling extension number

● Do Not Send Caller ID

9 On the SIP Settings tab, define authentication and registration settings for this SCP.



Signaling Control Point

Name:

Inbound Routing | Outbound Routing | SIP Settings

User Name:

Proxy Server:

Port: 5060

InboundOutbound Settings

This SCP will: ○ Receive registration from Contact

● Register with a Proxy/Registrar

Authentication Settings

□ Authentication Required

Authentication Name:

Password:

Verify Password:

Registration Settings

□ Registration Required

Registrar Server:

Registrar Port:

Preferred DTMF Transport: SIP INFO

Important! Wave determines the SCP for an incoming call by evaluating **User Name**, **Proxy Server**, **Port**, and **Local Listen Port**. When configuring SCPs, the combination of these four fields (described below and in step 16) cannot be the same for any two SCPs.

Enter the following information:

- **User Name**. 1-32 alphanumeric character name that identifies this SCP. Each SCP's user name must be unique and cannot match any user's extension. This field is only required if registration is required (see step 10).
- **Proxy Server**. ITSP address, or the address of another Wave Server to or from which this SCP is registering.
- **Port**. The default port number is 5060. This port is generally used for IP telephony, but if this port is in use in your system, you can specify another port.

10 In the Inbound \ Outbound section, specify whether the SIP destination endpoint requires authentication or registration, based on the requirements of your ITSP or SIP trunk provider. Typically, authentication and registration are required for third-party SIP servers.

- **This SCP will:** The setting you choose here depends on which of the following scenarios applies to you:
  - **This SCP is connecting to another Wave Server**. In a Wave Server-to-Wave Server configuration, you have 2 choices:
    - **If registration is required between the Wave Servers**, select **Receive registration from Contact** when configuring the SCP on one Server, and **Register with a Proxy/Registrar** when configuring the SCP on the other Server. It does not matter which setting you select on either Server, as long as the settings are different on each Server.
    - **If registration is not required between the Wave Servers**, select **Receive registration from Contact** when configuring the SCPs on both Servers, and then select **Not Required** in step 11.

    Go to step 11.
  - **This SCP is registering to an ITSP**. Select **Register with a Proxy/Registrar**, and go to step 12.

11 If you selected **Receive registration from Contact** in step 10, complete the following two sections:

a In the Authentication Settings section, select one of the following from the **Authentication** drop-down list:

- **Not Required**. Select this option if the SIP destination endpoint represented by this SCP does not requires authentication, for example a Wave Server-to-Wave Server configuration where registration is not required.
- **Custom**. Select this option to define SIP endpoint authentication settings specific to this SCP. For a description of how to use these settings, see “Setting up global SIP endpoint authentication parameters” on page 6-11.
- **Use SIP Defaults**. Select this option if this SCP uses the global SIP endpoint authentication settings you specified in “Setting up global SIP endpoint authentication parameters” on page 6-11.

b In the Registration Settings section, select the **Registration Required** checkbox if the SIP destination endpoint represented by this SCP requires registration.

Go to step 13.

12 If you selected **Register with a Proxy/Registrar** in step 10, complete the following two sections:

a In the Authentication Settings section, select the **Authentication Required** checkbox if the destination SIP endpoint requires authentication.

b For the following fields, enter the authentication credentials (**Authentication Name** and **Password**) provided by the remote SIP endpoint administrator. These three fields are disabled until you select any of the checkboxes in the previous step. These fields are required when they are enabled.

- **Authentication Name**. 1-32 alphanumeric characters. Authentication name cannot match an existing extension plus last name (for example, “Ryan605”), another SCP's authentication name, or the SIP global authentication name.
- **Password**. 1-48 characters.

  Note: The ^ and = special characters are not supported and will be ignored if you enter them in the **Password** field.

- **Verify Password**.

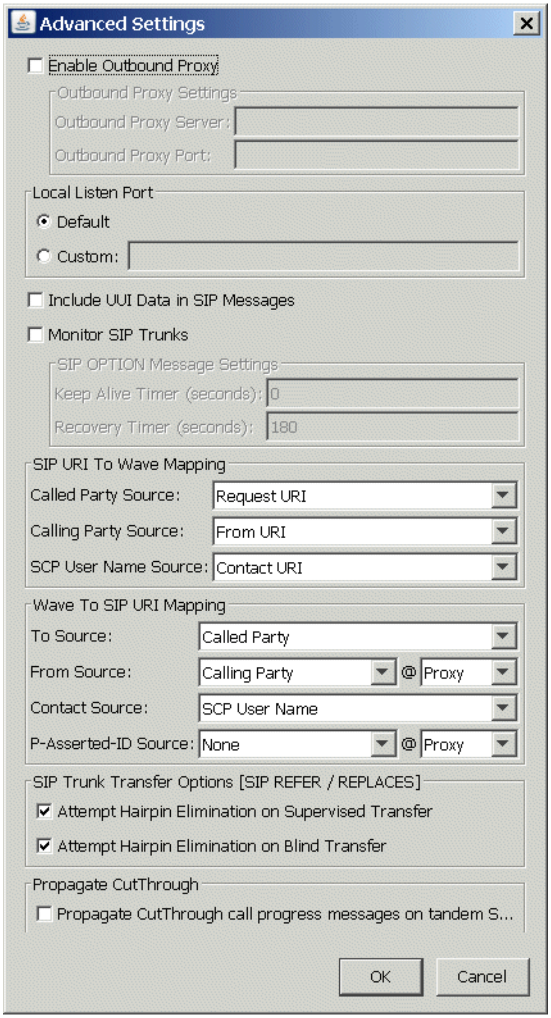
c In the Registration Settings section, select the **Registration Required** checkbox if the SIP destination endpoint requires registration. Then, enter the **Registrar Server** address and **Registrar Port** number provided by the remote SIP endpoint administrator.

13 Select one of the following from the **Preferred DTMF Transport** drop-down list, based on the requirements of your ITSP or SIP trunk provider:

- **Inband** (DTMF digits are left as tones in the original audio stream)
- **RFC 2833**
- **SIP INFO**

Note: This setting indicates a preference only - most ITSPs and SIP trunk providers use or prefer RFC 2833. If RFC 2833 is used by your ITSP or SIP trunk provider, Wave will automatically use RFC 2833, no matter what you specify here. On the other hand, if RFC 2833 is not supported by your ITSP or SIP trunk provider, Wave will use the setting that you specify here. If RFC 2833 is *not* supported by your ITSP or SIP trunk provider, select one of the other settings.

14 Click **Advanced Settings** to view or change this SCP's advanced settings. These settings are primarily used to fine-tune interoperability with ITSPs.



□ Enable Outbound Proxy

Outbound Proxy Settings

Outbound Proxy Server:

Outbound Proxy Port:

Local Listen Port

● Default

○ Custom:

□ Include UUI Data in SIP Messages

□ Monitor SIP Trunks

SIP OPTION Message Settings

Keep Alive Timer (seconds): 0

Recovery Timer (seconds): 180

SIP URI To Wave Mapping

Called Party Source: Request URI

Calling Party Source: From URI

SCP User Name Source: Contact URI

Wave To SIP URI Mapping

To Source: Called Party

From Source: Calling Party @ Proxy

Contact Source: SCP User Name

P-Asserted-ID Source: None @ Proxy

SIP Trunk Transfer Options [SIP REFER / REPLACES]

☑ Attempt Hairpin Elimination on Supervised Transfer

☑ Attempt Hairpin Elimination on Blind Transfer

Propagate CutThrough

□ Propagate CutThrough call progress messages on tandem S...

15 If this SCP connects to an ITSP that requires that you configure an outbound proxy server, select the **Enable Outbound Proxy** checkbox and then enter the following information in the Outbound Proxy Settings section.

- **Outbound Proxy Server**
- **Outbound Proxy Port**

16 The following settings define the default behavior of SIP trunks, and should not be modified unless you are directed to do so by your Vertical support representative.

- **Local Listen Port** settings
- **Include UUI Data in SIP Messages** checkbox
- **Monitor SIP Trunks** checkbox
- **SIP OPTION Message Settings**

17 The following settings are primarily used to fine-tune interoperability with ITSPs with respect to caller ID. You normally will not need to change the default values unless you are directed to do so by your Vertical support representative working in collaboration with your ITSP to resolve a specific issue.

Note: Domain source SIP message attribute mapping and P-Asserted-ID options described below may be required to support caller id and privacy related functions on some ITSPs.

- **SIP URI To Wave Mapping** settings:
  - **Called Party Source**.
  - **Calling Party Source**.
  - **SCP User Name Source.**
- **Wave To SIP URI Mapping** settings:
  - **To Source**.
  - **From Source** ___ @ ___. Select a value from the **Source** drop-down list, and then select one of the following from the @ drop-down list:
    - **Proxy.** This value represents the **Proxy Server** setting on the SIP Settings tab of the Signaling Control Point dialog. This is the default value.
    - **Wave IP**. This value represents the **SIP Local IP Address**. (To view or set this address, in IP Telephony, choose **Signaling Protocols > SIP**.).
  - **Contact Source**.
  - **P-Assisted-ID Source** ___ @ ___. Select a value from the P-Assisted ID Source drop-down, and then select one of the following from the @ drop-down list:
    - **Proxy.** This value represents the **Proxy Server** setting on the SIP Settings tab of the Signaling Control Point dialog. This is the default value.
    - **Wave IP**. This value represents the **SIP Local IP Address**. (To view or set this address, in IP Telephony, choose **Signaling Protocols > SIP**.).

18 Configure the **SIP Trunk Transfer Options [SIP REFER / REPLACES]** settings based on your ITSP's requirements. Select the following checkboxes if your ITSP expects a REFER request for transfers over SIP trunks. When these checkboxes are selected, after the transfer is completed the SIP trunk call is released by Wave. When these checkboxes are not selected, each transferred call uses 2 SIP trunks and Wave maintains control of the call.

Note: Typically you use the same setting for supervised and blind transfers. These settings are enabled by default.

- **Attempt Hairpin Elimination on Supervised Transfer**. When selected, Wave attempts to eliminate hair-pinning on SIP trunks for supervised transfers.
- **Attempt Hairpin Elimination on Blind Transfer**. When selected, Wave attempts to eliminate hair-pinning on SIP trunks for blind transfers.

The following list identifies the settings required by some ITSPs. If you are not sure how to configure these settings, contact your ITSP or Vertical support representative.

- **Verizon:** Select both checkboxes. Test and if transfers over SIP trunks do not work as expected, deselect both checkboxes.
- **AccessLine:** Dialect both checkboxes.
- **Broadvox:** Deselect both checkboxes.
- **CommPartners:** Select both checkboxes.
- **Cbeyond:** Select both checkboxes.

19 To enable propagate progress cut through, select the **Propagate CutThrough call progress messages on tandem SIP trunk calls** checkbox.

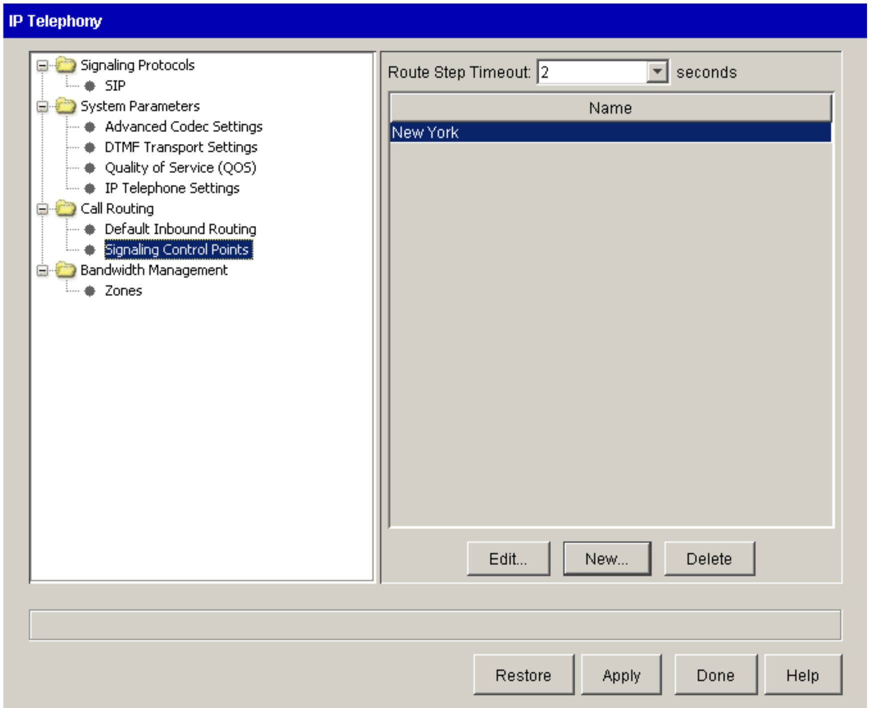
This option is required to support some ITSPs, and allows in-band call progress tones originating from an ITSP to be received by the calling party on a Wave phone before the call is answered.

- If this option is selected, the ITSP provides call progress tones to the calling party.
- If this option is not selected, Wave provides call progress tones.

If the setting is not correct, the calling party may not receive call progress tones as expected—and won't be able to tell if the called party is busy or ringing, or experience distorted or intermittent call progress tones.

20 Click **OK** to close the Advanced Settings dialog.

21 Click **OK** to add the SCP to the table.



Route Step Timeout: 2 seconds

Name
New York

22 Click **Apply** to save your changes.

Setting the route step timeout

You can adjust the amount of time that a Signaling Control Point step in an outbound routing table is given to operate before the system tries the next step in the table. Increasing this timeout (the maximum is 30 seconds) will help allow for network or other delays.

To set the Signaling Control Point route step timeout

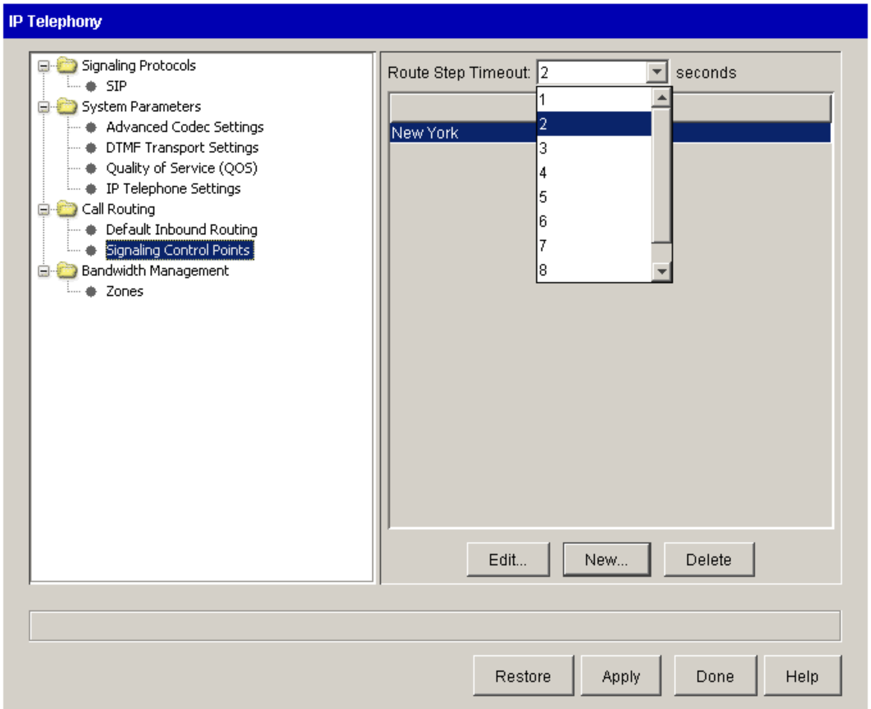
Click

1 If necessary, click the Administration tab of the Management Console.

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select **Signaling Control Points** from the Call Routing folder.

4 In the **Route Step Timeout** drop-down list, select the number of seconds before the system times out and tries the next step in an outbound call routing table.



Route Step Timeout: 2 seconds

Configuring default inbound IP call routing

To specify how to route incoming IP calls from unknown sources (that is, sources that are not included in your list of Signaling Control Points), configure the call handling rules with the default inbound call routing settings.

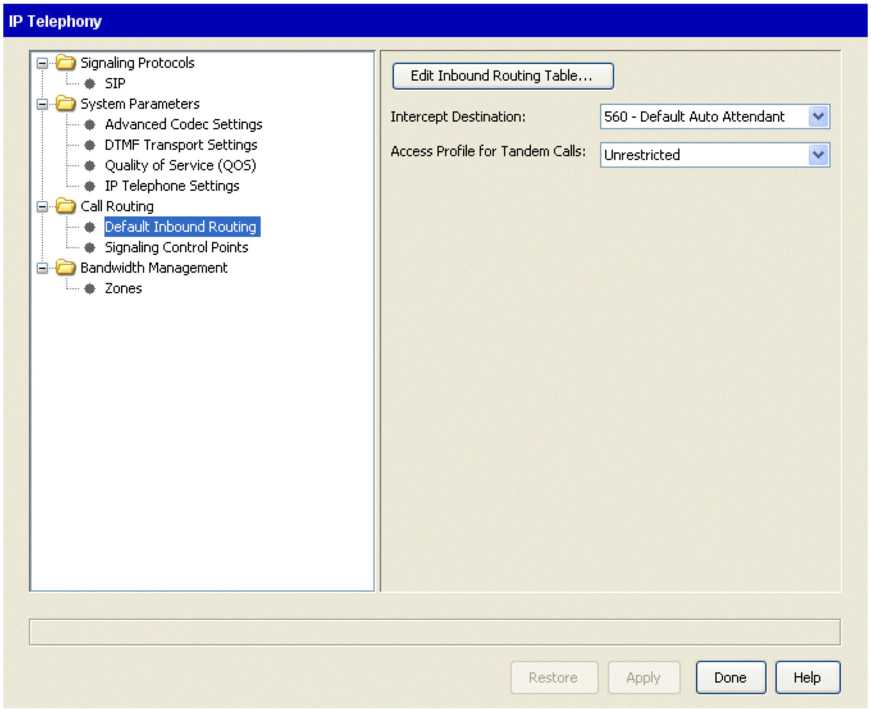
To configure default inbound IP call routing

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select **Default Inbound Routing** from the Call Routing folder.



Intercept Destination: 560 - Default Auto Attendant

Access Profile for Tandem Calls: Unrestricted

4 Click **Edit Inbound Routing Table** to specify the call sources, schedules, and routing.

For more information about editing the Inbound Routing Table, see “Configuring inbound routing tables” on page 8-4.

Note: If you want to route all incoming calls as received, there is no need to edit the inbound routing table. Only edit the inbound routing table if you want to route by schedule or do inbound digit translation.

5 Choose an extension from the **Intercept Destination** drop-down list.

6 Select an access profile in the **Access Profile for Tandem Calls** drop-down list.

7 Click **Apply** to save your changes.

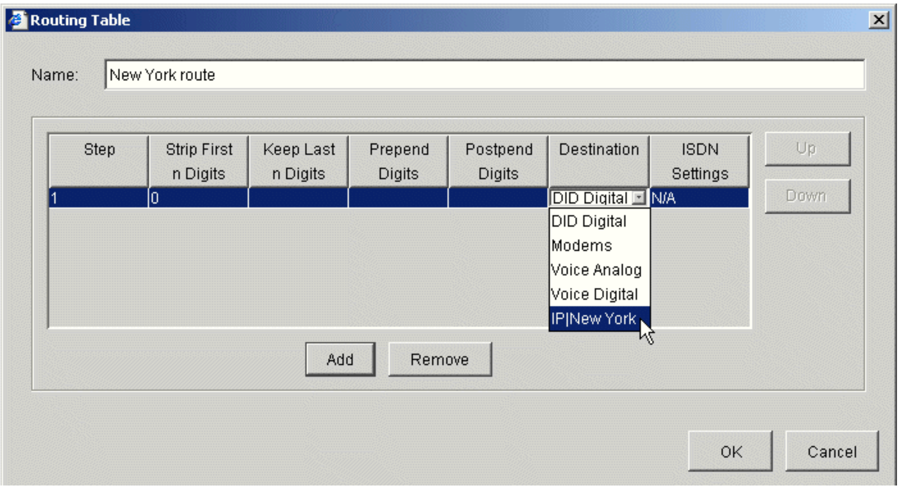
Including Signaling Control Points in the outbound call routing configuration

To route outbound calls to IP call destinations, select Signaling Control Points instead of trunk groups in your outbound call routing configuration.

To include Signaling Control Points in outbound call routing

While you are configuring your outbound call routing, select a Signaling Control Point from the **Destination** drop-down list at the point when a trunk group might be selected.

The following graphic shows an example of configuring an outbound routing table in the Outbound Routing applet:

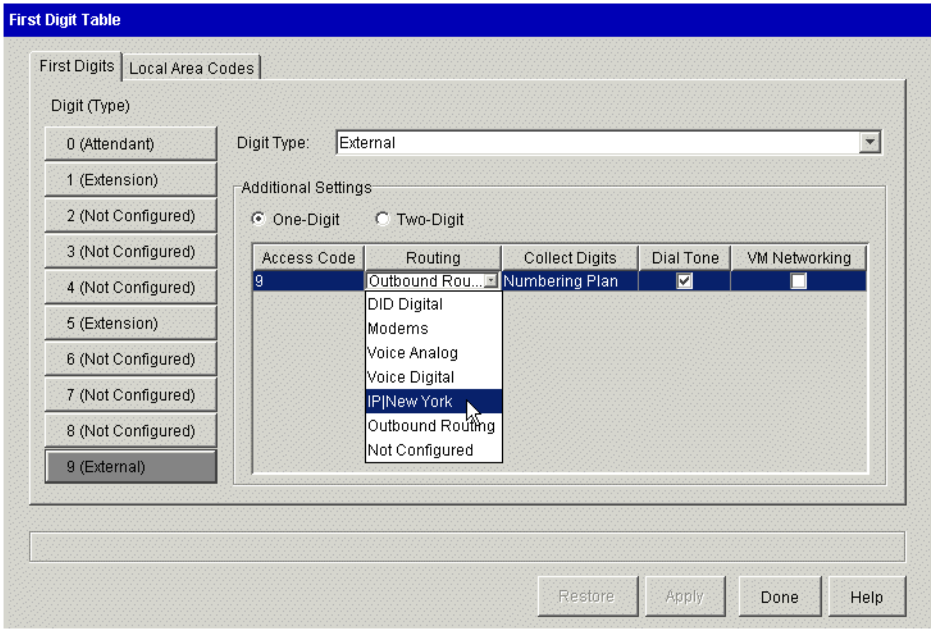


Routing Table

Name: New York route

Step	Strip First n Digits	Keep Last n Digits	Prepend Digits	Postpend Digits	Destination	ISDN Settings
1	0				DID Digital	N/A

The following graphic shows an example of configuring the External digit in the First Digit Table:



Digit Type: External

● One-Digit ○ Two-Digit

Access Code	Routing	Collect Digits	Dial Tone	VM Networking
9	Outbound Rou...	Numbering Plan	☑	□

Configuring SIP phones

This section provides instructions on configuring the desktop, wireless and software SIP phones certified for use with the Wave system. The procedures assume you are already familiar with configuring Wave digital phones, and only address the steps specific to configuring IP phone options.

SIP phones require the ability to log into and download files from the Wave FTP or TFTP server. Any network configurations that do not allow that connectivity will result in the SIP phones being unable to initialize. These configuration areas include, but are not limited to, the following:

- Incomplete routing
- External firewalls
- Internal firewalls, such as Check Point FireWall-1
- RRAS address / port filtering
- TFTP/FTP directory security

SIP phone configuration includes the following:

- Configuring SIP phone extensions
- Configuring Vertical-branded SIP phones
- Setting up OpenVPN Server for a Wave Gigabit-E SIP phone user
- Enabling IP call bandwidth
- Changing the password for the IPPhone user account

Configuring SIP phone extensions

This procedure assumes you are already familiar with configuring Wave phone extensions, and only addresses configuration tasks specific to configuring SIP phone extensions.

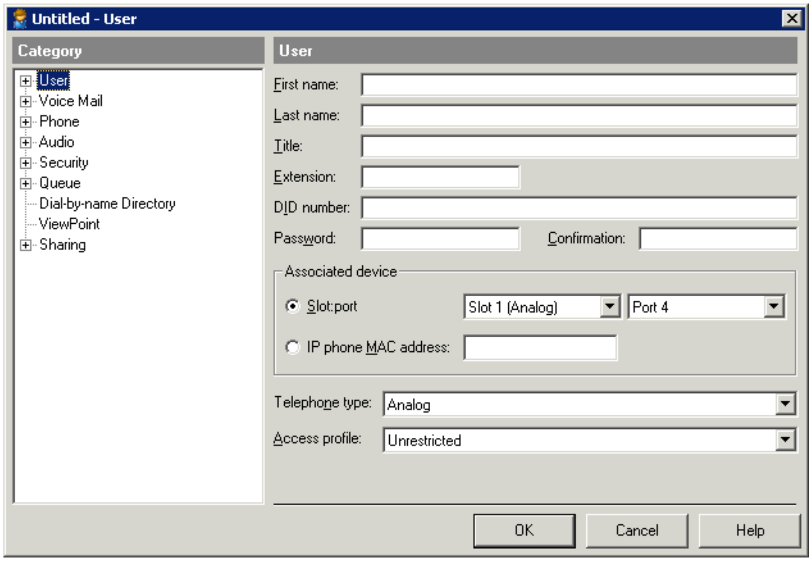
To configure SIP phone extensions

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section. The User/Group Management applet opens, with the Users view showing.

3 Double-click the user to whom you want to assign a SIP phone extension, or create a new SIP phone user. The User dialog opens.



Untitled - User

Category

- User
- Voice Mail
- Phone
- Audio
- Security
- Queue
- Dial-by-name Directory
- ViewPoint
- Sharing

User

First name:

Last name:

Title:

Extension:

DID number:

Password: Confirmation:

Associated device

● Slot:port Slot 1 (Analog) Port 4

○ IP phone MAC address:

Telephone type: Analog

Access profile: Unrestricted

4 Click **IP phone MAC Address** field, and then enter the phone's MAC address. The phone's MAC address can be found on the phone itself, on the box the phone came in, or via the phone's options menu.

5 Choose the appropriate **Telephone type** from the drop-down list. Do one of the following:

- For a Vertical-branded SIP phone, select the appropriate model.
- For a third-party SIP phone device (for example, a Counterpath SIP softphone), select **IP third party SIP Telephone**.

6 Click **OK** to save the settings.

- If you are configuring Vertical-branded SIP phones, go to the next section.
- If you are configuring a third-party SIP phone device, see the documentation that came with the device for additional configuration requirements.

Configuring Vertical-branded SIP phones

The configuration process for Vertical-branded SIP phones is similar to that of digital phones, as described in Chapter 10. This section describes the following additional configuration tasks specific to Vertical branded SIP phones. For tasks that apply to your configuration, perform the indicated steps at each Vertical-branded SIP phone. Be sure to follow the steps for your specific phone model.

- **Optional:** Configuring a static IP address for Vertical-branded SIP phones. See page 6-32.
- **Required:** Configuring the TFTP server to synchronize Vertical-branded SIP phones with the Wave Server. See page 6-33.
- **Optional:** Setting date and time on Vertical-branded SIP phones. See page 6-34.

Configuring a static IP address for Vertical-branded SIP phones

This task is optional, depending on how you want to assign an IP address to a Vertical-branded SIP phone.

- By default, a Vertical-branded SIP phone’s IP address is dynamically assigned via DHCP. If you want to continue using this default method, go to the next section, “Configuring the TFTP server to synchronize Vertical-branded SIP phones with the Wave Server” on page 6-33.
- If you want to assign a static IP address to the phone, perform the steps below on all Vertical branded SIP phones. Be sure to perform the steps specific to your phone model.

1 To configure a static IP address on a Vertical-branded 9133i, 9112i, 480i, or 480i/CT SIP phone:

a Press the Options button.

b Select **Network Settings** from the main menu. When prompted, enter the password (the default password is 22222.)

c Go to step 3.

2 To configure a static IP address on a Vertical-branded 53i, 55i, or 57i SIP phone:

a Press the Options button.

b Select **Administrator Menu**. When prompted, enter the admin password (the default password is 22222.)

c Select **Network Settings > DHCP Settings**.

3 Select **DHCP > Use DHCP?**

4 Select **No**, and then press **Done**.

5 Select and configure the settings for the phone’s IP address, Subnet Mask, and Gateway.

Configuring the TFTP server to synchronize Vertical-branded SIP phones with the Wave Server

This task is required. You must perform the following steps on all Vertical branded SIP phones. Be sure to perform the steps specific to your phone model.

1 To configure the TFTP server on a Vertical-branded 9133i, 9112i, 480i, or 480i (CT) SIP phone:

a Press the Options button.

b Select **Network Settings** from the main menu. When prompted, enter the password (the default password is 22222.)

c Select the TFTP server options, and then select **TFTP Server > Primary TFTP**.

d Go to step 3.

2 To configure the TFTP server on a Vertical-branded 53i, 55i, and 57i SIP phone:

a Press the Options button.

b Select **Administrator Menu**. When prompted, enter the admin password (the default password is 22222.)

c Select the TFTP server options, and then select **TFTP Server > Primary TFTP**.

3 Enter the VAM IP address on the Wave Server. (The factory-default VAM IP address is 192.168.205.1.)

4 Press **Done** (or **Cancel**). Continue pressing **Done** until you are asked to restart the phone, and then confirm the phone restart. If you are not prompted to restart the phone, manually restart the phone by pressing the Options menu and then selecting **Phone Status > Restart Phone**.

Note: The phone may take several minutes to download required configuration files, and restart automatically one or more times depending on which files are required.

Setting date and time on Vertical-branded SIP phones

This task is optional. By default, after a SIP phone downloads the configuration file the date and time displayed on the phone is set to the physical location of the Wave Server server. If the SIP phone is in a different time zone than the Wave server, the phone's date and time may not match the user's location. This section describes how to adjust the date and time displayed on the phone.

To set date and time

1 Press the **Options** button.

2 Scroll to **Date and Time** and press **Show**.

3 Select **Time Server** and press **Show**. Enter the IP address of the Wave Server, and then press **Done**.

4 Select **Set Time** and press **Show**. Enter the current time, and then press **Done**.

5 Select **Time Format** and press **Show**. Select either **12h** or **24h**, and then press **Done**.

6 Select **Set Date** and press **Show**. Enter current date, and then press **Done**.

7 Select **Date Format** and press **Show**. Select the preferred date style, and then press **Done**.

8 Select **Time Zone** and press **Show**. Select your time zone, and then press **Done**.

9 Select **Daylight Savings** and press **Show**. Select the correct daylight savings time setting, and then press **Done**.

10 When the Date and Time settings are complete, press **Done**.

Setting up OpenVPN Server for a Wave Gigabit-E SIP phone user

Wave OpenVPN Server is the preferred method to enhance remote phone integration. OpenVPN Server allows phones outside of your network to behave the same as local phones. With OpenVPN Server, when a remote user goes off-hook, the user’s phone automatically connects to your network. The OpenVPN Server extends your private network and its resources to support remote users with all the functionality and security available to local users.

OpenVPN Server is supported on the following Wave Gigabit-E SIP phones, which include a built-in virtual private network client. This client uses the OpenVPN protocol to support a secure connection to the Wave Server.

- Vertical IP Edge 5000i-LLCDG large LCD screen phone
- Vertical IP Edge 5000i-24G 24-button phone

Important! Before setting up OpenVPN Server for a user as described in this section, you must install and configure OpenVPN Server on the Wave Server. See “Configuring Wave OpenVPN Server” on page 6-61.

This section describes how to set up OpenVPN Server for each Wave Gigabit-E SIP phone user via User/Group Management. You may also need to configure each user’s SIP phone itself, depending on how you choose to address the security concerns described below.

Security concerns when configuring a user’s VPN credentials

There are two ways to configure the user’s VPN credentials:

- **Via User/Group Management**. This method is easier for the Wave administrator, because the user name and password can be supplied at the same time that VPN is enabled for the user, as described below. However, this method is less secure because the credentials will be sent to the phone through the TFTP server which is inherently not secure. If there are any security concerns, configure the user’s VPN credentials using the phone.
- **Via the phone itself**. This requires some extra effort on the part of the end user, but is more secure. See Chapter 3 in the *Wave OpenVPN Server Guide* for detailed steps.
    - If you enter the user’s VPN credentials via User/Group management, you do not need to perform any further configuration on the user’s phone.
    - If you configure the user’s VPN credentials on the phone, you still need to enable OpenVPN Server for the user as described below.

Important! Phones to be used with OpenVPN Server must first be staged locally on a Wave Server running Wave 4.0. This will allow the 4.0 firmware that supports the latest VPN features to be downloaded to the phones, so that future firmware upgrades will be able to be downloaded via VPN itself.

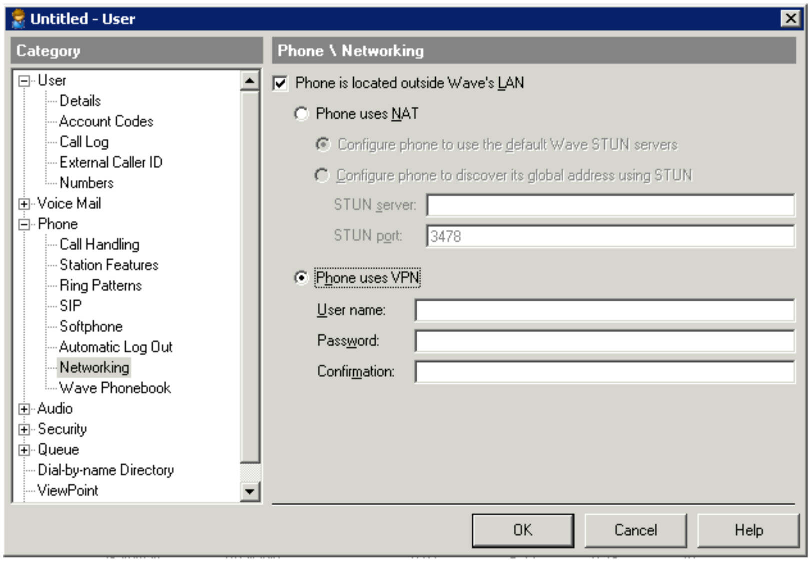
To enable VPN for a user

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Edit the user, and select **Phone > Networking** in the left pane.



☑ Phone is located outside Wave's LAN

○ Phone uses NAT

● Configure phone to use the default Wave STUN servers

○ Configure phone to discover its global address using STUN

STUN server:

STUN port: 3478

● Phone uses VPN

User name:

Password:

Confirmation:

4 Select the **Phone is located outside Wave's LAN** checkbox.

5 Click **Phone uses VPN**.

6 Enter a **User name** and **Password** combination that you created as described in “Adding users” in Chapter 2 in the *Wave OpenVPN Server Guide*.

Important! If you have any security concerns, enter these credentials directly on the phone itself, as described in “Configuring VPN on a user’s SIP phone” in Chapter 3 in the *Wave OpenVPN Server Guide*.

7 Click **OK** to save your changes for this user.

Setting up NAT traversal for a user

NAT traversal is one method to enhance remote phone integration. NAT traversal is less secure than Wave OpenVPN Server, the preferred method, but is supported on all Vertical Edge SIP phones. (For more about Wave OpenVPN Server, see "Configuring Wave OpenVPN Server" on page 6-61.)

NAT traversal is a way to establish and maintain IP connections that traverse network address translation (NAT) gateways. NAT provides automated translation of IP addresses between different networks. For example, a company might use private IP addresses on a LAN that are represented by a single IP address on the WAN side of their router.

Configuring NAT traversal consists of the following tasks in the following order:

- **Configuring the Wave Server**
- **Configuring remote users** for NAT traversal, described below
- **Configuring your router**

Important! Before configuring NAT traversal for a user as described in this section, you must configure NAT traversal on the Wave Server. See "Configuring NAT traversal" on page 6-64 for more about Wave Server and router configuration requirements.

To configure NAT traversal for a remote user

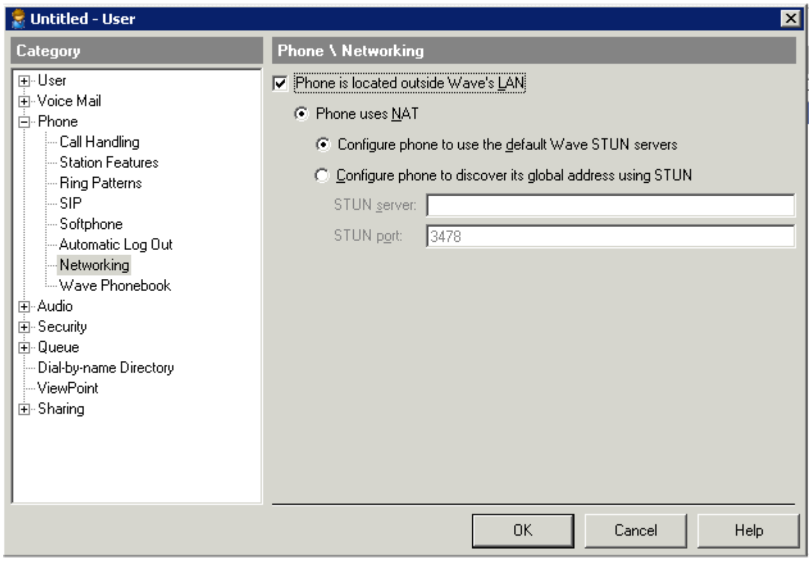
Perform the following step for each Wave user with a remote SIP phone (a SIP phone that is outside your Wave network).

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Edit the user, and select **Phone > Networking** in the left pane.



☑ Phone is located outside Wave's LAN

● Phone uses NAT

● Configure phone to use the default Wave STUN servers

○ Configure phone to discover its global address using STUN

STUN server:

STUN port: 3478

4 Select the following options:

- **Phone is located outside Wave's LAN**
- **Phone uses NAT**

5 Select one of the following:

- **Configure phone to use the default Wave STUN servers**. Select this option if you want this user to use the STUN servers that you specified via IP Telephony. In most cases, you should select this option.
- **Configure phone to discover its global address using STUN**. Select this option if you want this user to use a different STUN server, then specify that STUN server's IP address or hostname.

6 Click **OK** to save the user.

Enabling IP call bandwidth

SIP phones cannot make external calls until the bandwidth is allocated for them. To do this, configure the Home bandwidth management zone in "Configuring the home zone" on page 6-41.

Changing the password for the IPPhone user account

The IPPhone account is not used unless FTP access required. For security reasons, Vertical Communications recommends that you change the password for the IPPhone user account from the default password of Vertical4VoIP!

To change the password for the IPPhone user account

1. Log on to the Management Console.
2. Open the Password Administration applet.
3. In the Password Administration dialog, click the IPPhone user account and click **Edit**.
4. Enter the new password in the **Password** and **Confirm Password** fields.
5. Click **OK**.
6. Click **Done**.

Configuring bandwidth management zones

Configure the home, remote and default remote zones using the procedures in this section. For information about the bandwidth management zones, see “Bandwidth management” on page 28-10.

Review the following topics to configure bandwidth management zones

- Zone configuration recommendations
- Codec negotiation
- Configuring the home zone
- Configuring remote zones
- Configuring the remote default zone

Zone configuration recommendations

Keep in mind the following rules while configuring bandwidth management zones:

- A bandwidth management zone is defined by a set of IP address ranges. Any number of Signaling Control Points (SCPs) and IP phones can exist in the same zone. Any SCP or IP phone whose IP address is not explicitly configured as part of a zone is automatically included in the Default Zone. All TDM devices, including voicemail ports and conference bridges reside in the Home Zone.
- For devices in two different bandwidth management zones to be able to communicate, it is necessary that a common codec is configured in each of the zones' inter-zone preference lists. In the absence of a common codec, calls between the two zones will not be allowed.
- Calls between bandwidth management zones always engage the inter-zone rules for both zones.
- When an IP device is involved in a conference, the inter-zone rules between the IP device's zone and the Home Zone come into play. If there are no common codecs, or there is insufficient bandwidth, then the device is not permitted to participate in the conference.

Codec configuration guidelines

With the rules listed above in mind, Vertical recommends that you follow these configuration guidelines:

- Configure all zones to use the G.711U codec only (either u-law, a-law, or both), and remove the G.729 codec from the inter-zone codec preference lists. If G.729 or G.711A is specifically required in your implementation, use then that codec only and leave all other codecs off the preference lists.
- If there is a zone requiring G.729 exclusively, then G.711 should be left off of its inter-zone preference list. In this situation, it is essential that all remaining zones include G.729 on their inter-zone codec preference lists. Devices in zones configured to use G.711 exclusively will not be able to call devices in zones configured to use G.729 exclusively.

Codec negotiation

Wave chooses a codec based on the following rules:

- All codecs not supported by both endpoints are filtered out.
- The remaining codecs are scored based on their positions in the preference lists (for example, if G.711 is first on one list and third on the other, its score is 4).
- Wave chooses the codec with the lowest score.
  - If two codecs have the same score, Wave prioritizes lower bandwidth over voice quality.
  - If G.711 Mu-Law and G.711 A-Law tie for the lowest score, Wave uses Mu-Law.

Configuring the home zone

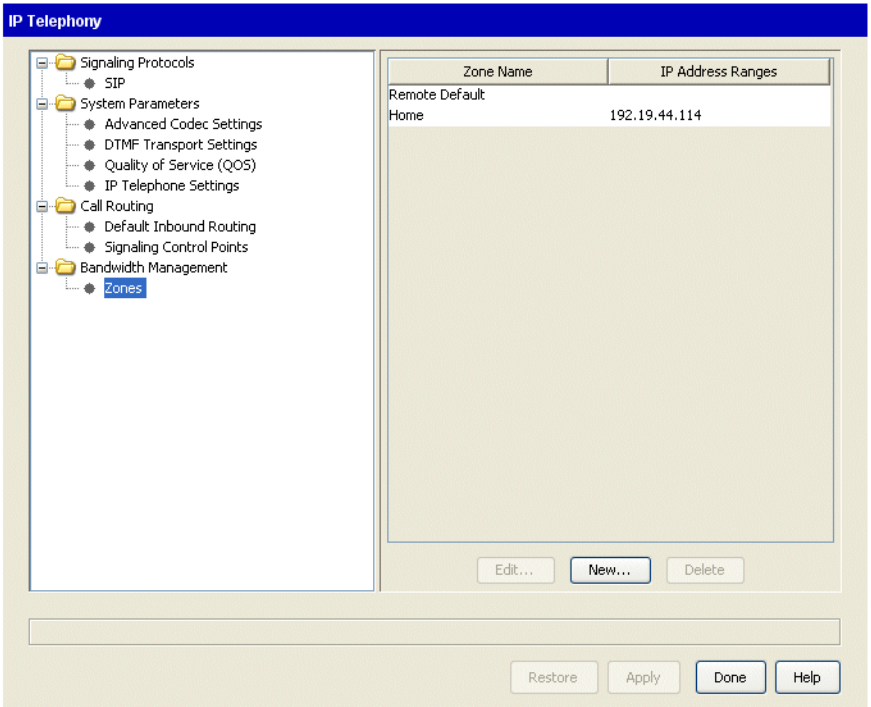
To configure the home zone

1 If necessary, click the Administration tab of the Management Console.

Click

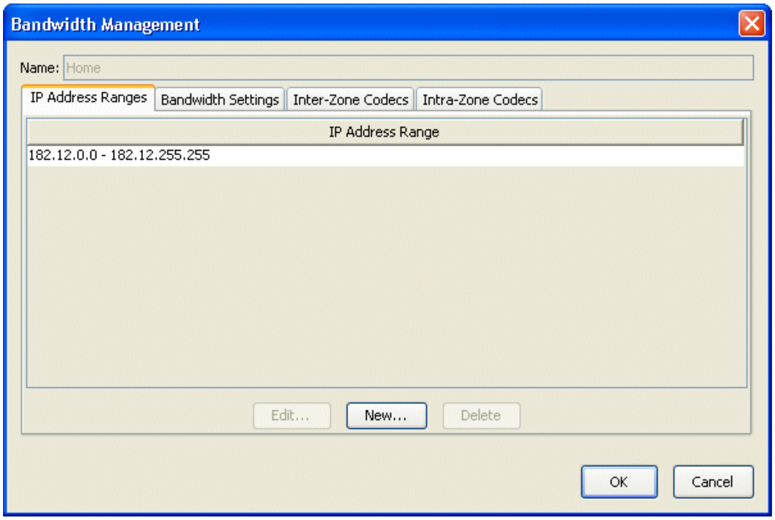
2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Zones from the Bandwidth Management folder.



Zone Name	IP Address Ranges
Remote Default	
Home	192.19.44.114

4 Select **Home** from the table, and click **Edit**.



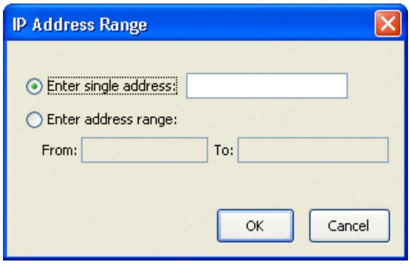
5 Configure the IP address range.

Include all the applicable IP address ranges used by the IP phones on the local Wave system. The Home Zone always includes the IP address of the Wave for bandwidth and call control purposes, whether or not it is explicitly specified in the IP Telephony applet.

To add an IP address range:

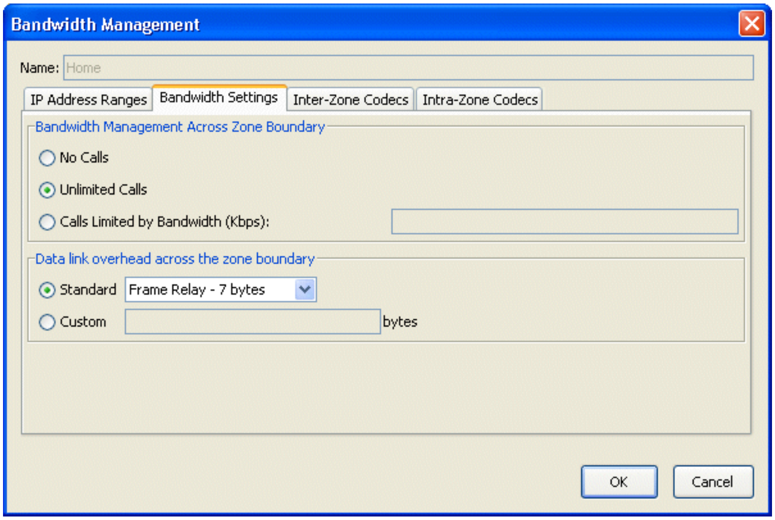
a Select the IP Address Ranges tab.

b Select the IP address range and click **Edit** to alter the existing range, or click **New** to add a new IP address range.



You can also add single IP addresses.

6 Click the Bandwidth Settings tab.



Name: Home

Bandwidth Management Across Zone Boundary

○ No Calls

● Unlimited Calls

○ Calls Limited by Bandwidth (Kbps):

Data link overhead across the zone boundary

● Standard Frame Relay - 7 bytes

○ Custom bytes

a Select a **Bandwidth Management Across Zone Boundary** setting.

- **No Calls**. No calls are allowed to IP addresses outside the ranges defined in this zone.
- **Unlimited Calls**. All calls to or from all IP addresses are allowed.
- **Calls Limited by Bandwidth (Kbps)**. Calls placed to or received from IP addresses outside this zone are limited to the number that can be supported by the bandwidth specified here.

b Select a **Data link overhead across the zone boundary** setting.

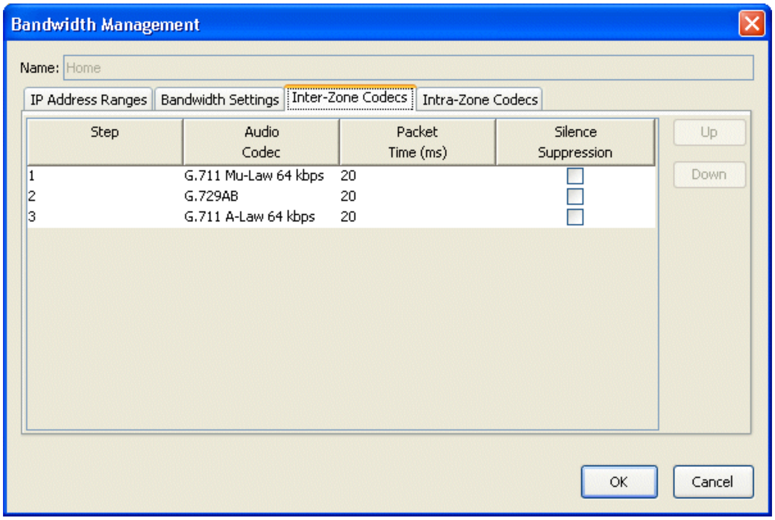
- **Standard**. Select one of the standard data links from the drop-down list. The option you select determines the amount of overhead the system adds to the bandwidth when calls cross the zone boundary. Specifying enough overhead is important in preventing too many calls from being placed over the WAN link; if the transport overhead is not included, then more calls would be allowed than the link could support.

Note: Be sure to use the option that most accurately reflects the type of data link used in this zone. If you need to use a different value than those provided, enter the value in the **Custom ___ bytes** field, described below.

- **Custom ___ bytes**. Enter a custom data link overhead in the field provided.

Note: This helps the Wave system calculate Inter-zone bandwidth availability for IP calls. This setting must be changed if the physical data link type across this zone is changed.

7 Click the Inter-Zone Codecs tab.



Name: Home

Step	Audio Codec	Packet Time (ms)	Silence Suppression
1	G.711 Mu-Law 64 kbps	20	□
2	G.729AB	20	□
3	G.711 A-Law 64 kbps	20	□

The default codecs are displayed in a table. Depending on your ITSP's specific requirements, you may need to change the default settings for a codec, add or remove a codec, and so forth.

a To change the default settings for a codec:

- **Packet Time (ms)**. Click in this column for the codec and then select the value to use from the drop-down list.

  Note: This setting indicates a preference only, and may be overridden automatically depending on other factors. For example, if more than 48 channels are configured on the Wave Server base unit, or more than 64 channels are configured on a Media Resource Module (MRM), a packet time of 30 ms will be used to support the total number of channels, regardless of what value you specify here.

- Select or deselect the **Silence Suppression** checkbox for the codec to enable or disable silence suppression.

b To add a codec, click **Add**. A new entry is added at the bottom of the table. Specify the following:

- **Audio Codec**. Click in this column and then select an available codec name to add from the drop-down list.

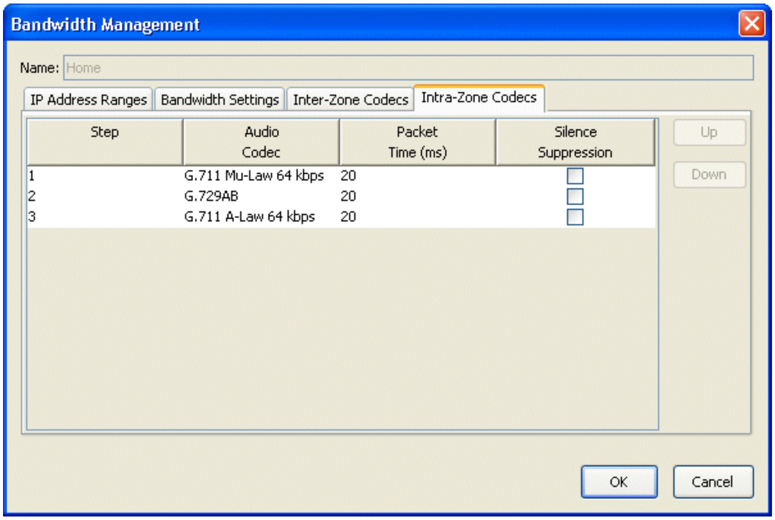
See step 7a for more about the following settings:

- **Packet Time (ms)**.
- **Silence Suppression**.

c To change a codec’s position in the list, select it and then click **Up** or **Down**.

d To remove a codec from the list, select it, and then click **Remove**.

8 Click the Intra-Zone Codecs tab. To define intra-zone codec behavior, see step 7 for actions you can perform here.



Name: Home

Step	Audio Codec	Packet Time (ms)	Silence Suppression
1	G.711 Mu-Law 64 kbps	20	□
2	G.729AB	20	□
3	G.711 A-Law 64 kbps	20	□

9 Click **OK** to close the Bandwidth Management dialog.

10 Click **Apply** to save the Home zone configuration.

Configuring remote zones

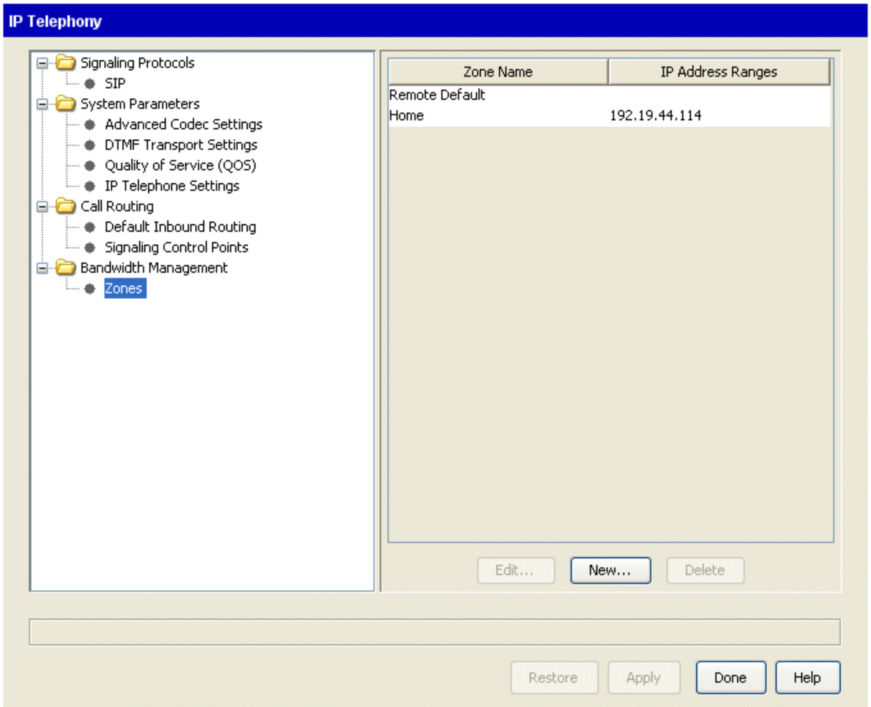
To configure remote zones

1 If necessary, click the Administration tab of the Management Console.

Click

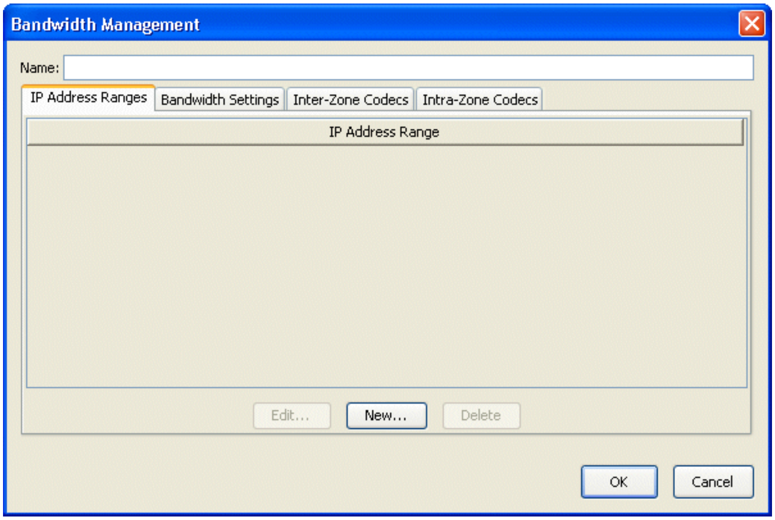
2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Zones from the Bandwidth Management folder.



Zone Name	IP Address Ranges
Remote Default	
Home	192.19.44.114

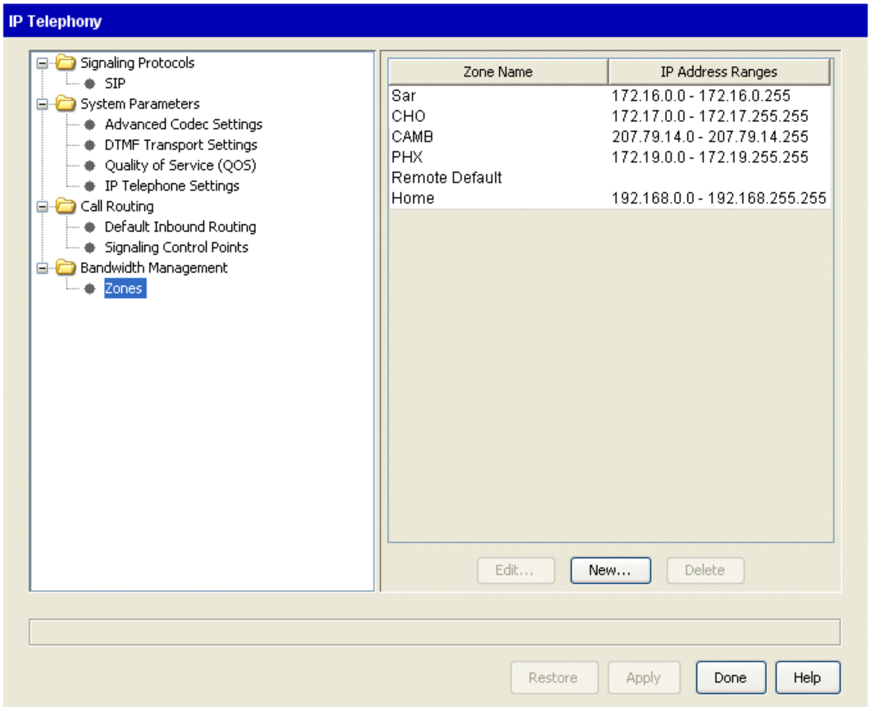
4 Click **New** to open the Bandwidth Management dialog.



5 Enter a **Name** for the zone.

6 Configure the IP address ranges, bandwidth settings, inter-zone codecs, and intra-zone codecs as explained in “Configuring the home zone” on page 6-41.

7 Click **OK** to close the Bandwidth Management dialog. The new zone is displayed in the list.



Zone Name	IP Address Ranges
Sar	172.16.0.0 - 172.16.0.255
CHO	172.17.0.0 - 172.17.255.255
CAMB	207.79.14.0 - 207.79.14.255
PHX	172.19.0.0 - 172.19.255.255
Remote Default	
Home	192.168.0.0 - 192.168.255.255

8 Click **Apply** to save the new remote zone configuration.

Configuring the remote default zone

To configure the remote default zone

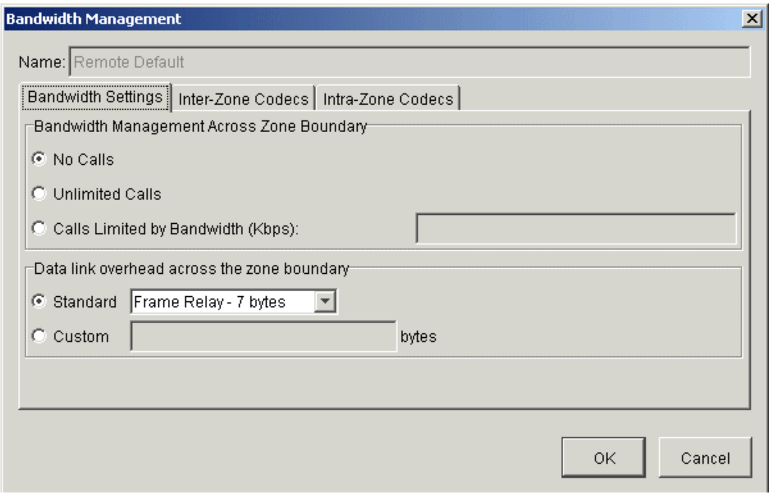
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Zones from the Bandwidth Management folder.

4 Select **Remote Default** from the table, and click **Edit**.



Bandwidth Management

Name: Remote Default

Bandwidth Management Across Zone Boundary

● No Calls

○ Unlimited Calls

○ Calls Limited by Bandwidth (Kbps):

Data link overhead across the zone boundary

● Standard Frame Relay - 7 bytes

○ Custom bytes

5 Configure the bandwidth settings, inter-zone codecs, and intra-zone codecs as explained in “Configuring the home zone” on page 6-41.

Note: For security reasons the default **Bandwidth Management Across Zone Boundary** setting is No Calls.

Note: You do not configure IP address ranges in the Remote Default zone configuration because this zone is used to manage bandwidth for all calls from IP addresses not defined in any of your configured zones.

6 Click **OK** to close the Bandwidth Management dialog.

7 Click **Apply** to save the remote zone configuration changes.

Configuring music on hold for IP calls

To configure music on hold for IP calls, perform the following tasks:

- **Allocate low bit rate music on hold resources.** Low Bit Rate (G.729A/G.711) music on hold resources are *required* if IP calls are expected to use the G.729 codec. If IP calls are expected to use the G.729 codec and no low bit rate resources are allocated for music on hold, IP callers on hold will hear silence instead of music

  To allocate low bit rate music on hold resources, use the Resource Management applet or Resource Management Advisor as described in “Using the Resource Management applet and Resource Management Advisor” on page 23-45.

- **Configure a system port for music on hold and enable system-wide music on hold.** See “Configuring Music On Hold” on page 16-21. Be sure to select the **Support IP Music On Hold** checkbox when you enable system-wide music on hold.

Adjusting IP call quality parameters

Caution! *These parameters only apply to the IP telephony resources on the Wave system and do not affect the performance of the IP phones. These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

Most of the IP call quality parameters can be found in the System Parameters folder of the IP Telephony applet. If you are not familiar with IP telephony, you should contact your Wave product support vendor for information about adjusting these settings. If you want to return to the system defaults, click Restore Defaults in any of the System Parameters screens.

You can adjust the following IP call quality parameters:

- Jitter buffer. See page 6-53.
- Echo cancellation. See page 6-54.
- Comfort noise. See page 6-56.
- Gain. See page 6-57.
- DTMF transport settings. See page 6-59.
- Quality Of Service (QoS) settings. See page 6-60.

Jitter buffer

Caution! *This is an expert setting that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

Voice packets can experience a high level of network delay, especially if the lines are congested. The jitter buffer temporarily holds incoming packets in order to assemble them in the correct order and recreate a high-quality voice signal.

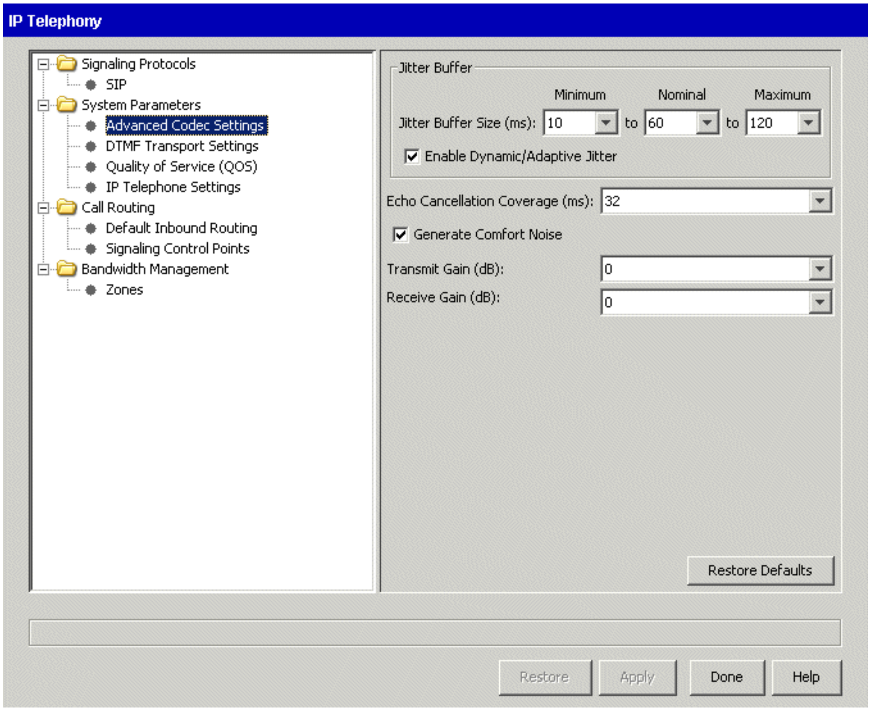
To adjust the jitter buffer

Click

1 If necessary, click the Administration tab of the Management Console.

2 Click the IP Telephony icon, located in the PBX Administration section.

3 In the left pane, expand System Parameters and then click Advanced Codec Settings.



Jitter Buffer

	Minimum		Nominal		Maximum
Jitter Buffer Size (ms):	10	to	60	to	120

☑ Enable Dynamic/Adaptive Jitter

Echo Cancellation Coverage (ms): 32

☑ Generate Comfort Noise

Transmit Gain (dB): 0

Receive Gain (dB): 0

4 Specify the range of acceptable delay in the **Jitter Buffer Size** drop-down lists.

5 Select the **Enable Dynamic/Adaptive Jitter** checkbox (this is the default setting).

The Dynamic/Adaptive Jitter feature optimizes the jitter buffer based on voice traffic and network conditions. If you disable this feature, the Wave system adheres to the values in the Nominal and Maximum fields.

6 Click **OK**.

Echo cancellation

Caution! *This is an expert setting that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

Echo in a phone network is caused by signal reflections generated by the hybrid circuit that converts between a 4-wire circuit (a separate transmit and receive pair) and a 2-wire circuit (a single transmit and receive pair). Echo is present even in a conventional circuit switched phone network. However, it is acceptable because the round trip delays through the network are smaller than 5 ms and the echo is masked by the normal side tone every phone generates.

Perceived echo becomes a problem in packet-switched networks because the round trip delay through the network is almost always greater than 5 ms. Thus, echo cancellation techniques are often used.

Echo is generated toward the packet-switched network from the TDM phone network. The echo canceller compares the voice data received *from* the packet-switched network with voice data being transmitted *to* the packet-switched network. The echo from the phone network hybrid is removed by a digital filter on the transmit path into the packet-switched network.

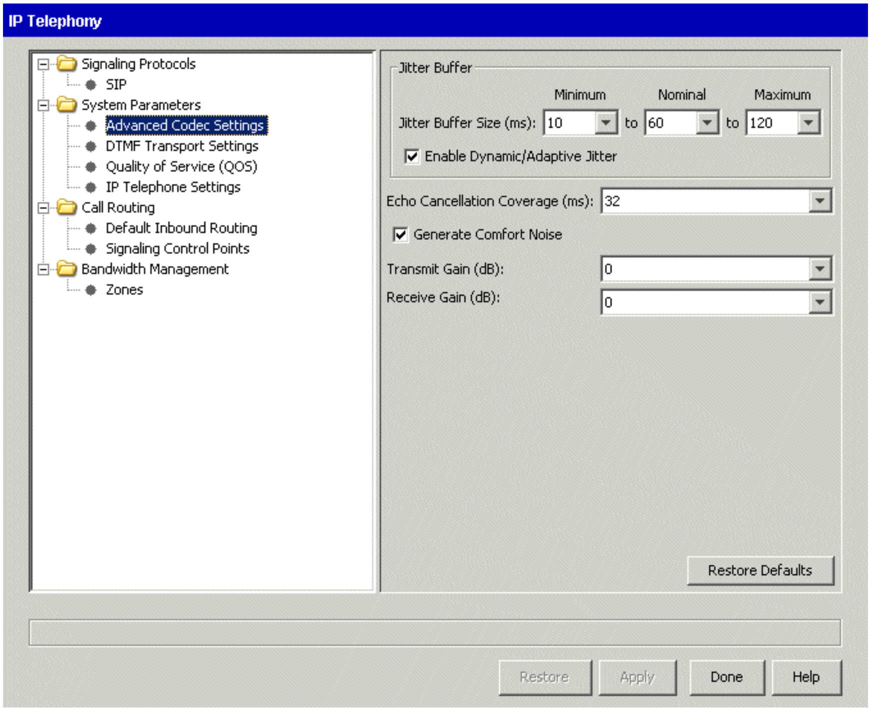
To adjust the echo cancellation settings

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 In the left pane, expand System Parameters and then click Advanced Codec Settings.



Jitter Buffer

	Minimum		Nominal		Maximum
Jitter Buffer Size (ms):	10	to	60	to	120

☑ Enable Dynamic/Adaptive Jitter

Echo Cancellation Coverage (ms): 32

☑ Generate Comfort Noise

Transmit Gain (dB): 0

Receive Gain (dB): 0

4 Select a value from the **Echo Cancellation Coverage** drop-down list.

Note: The recommended value (and default) is 32 ms.

5 Click **OK**.

Comfort noise

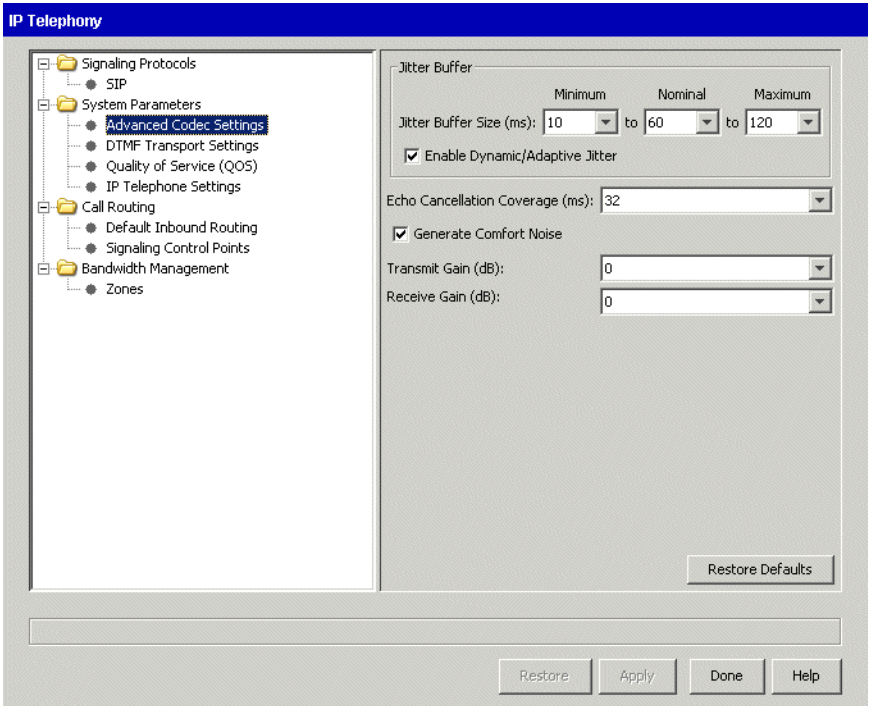
Caution! *This is an expert setting that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

This option generates comfort noise during silences on the receiving end of the phone call in calls where silence suppression is enabled. Comfort noise is white noise that masks “dead” time in a phone conversation. Use this option to simulate a circuit-switched phone conversation. This option is enabled by default.

To adjust the comfort noise settings

Click

1. If necessary, click the Administration tab of the Management Console.
2. Click the IP Telephony icon, located in the PBX Administration section.
3. In the left pane, expand System Parameters and then click Advanced Codec Settings.



Jitter Buffer Size (ms): 10 to 60 to 120

☑ Enable Dynamic/Adaptive Jitter

Echo Cancellation Coverage (ms): 32

☑ Generate Comfort Noise

Transmit Gain (dB): 0

Receive Gain (dB): 0

4 Select the **Generate Comfort Noise** checkbox if you want the Wave Server to automatically generate background noise.

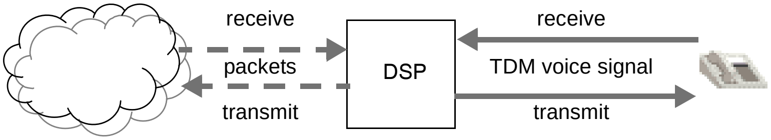
5 Click **OK**.

Gain

Caution! *This is an expert setting that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

The gain settings adjust the transmit gain and receive gain levels for the TDM segment of a call.

The following diagram shows transmit and receive gain:



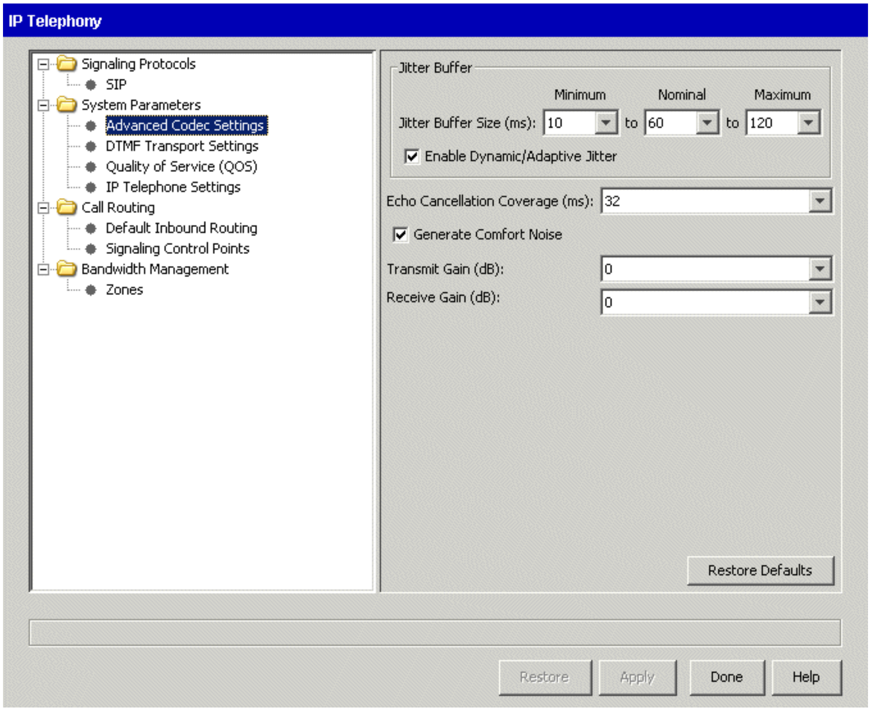
To adjust the transmit and receive gain values

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 In the left pane, expand System Parameters and then click Advanced Codec Settings.



IP Telephony

Jitter Buffer

	Minimum		Nominal		Maximum
Jitter Buffer Size (ms):	10	to	60	to	120

☑ Enable Dynamic/Adaptive Jitter

Echo Cancellation Coverage (ms): 32

☑ Generate Comfort Noise

Transmit Gain (dB): 0

Receive Gain (dB): 0

4 Adjust the following values.

- **Transmit Gain**. If the volume level to the TDM phone is too low, you can increase the transmit gain.
- **Receive Gain**. If the volume level from the TDM phone is too low, you can increase the receive gain.

5 Click **OK**.

DTMF transport settings

Caution! *The default values in this pane will work for most VoIP networks. These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative to address specific VoIP network requirements or issues.*

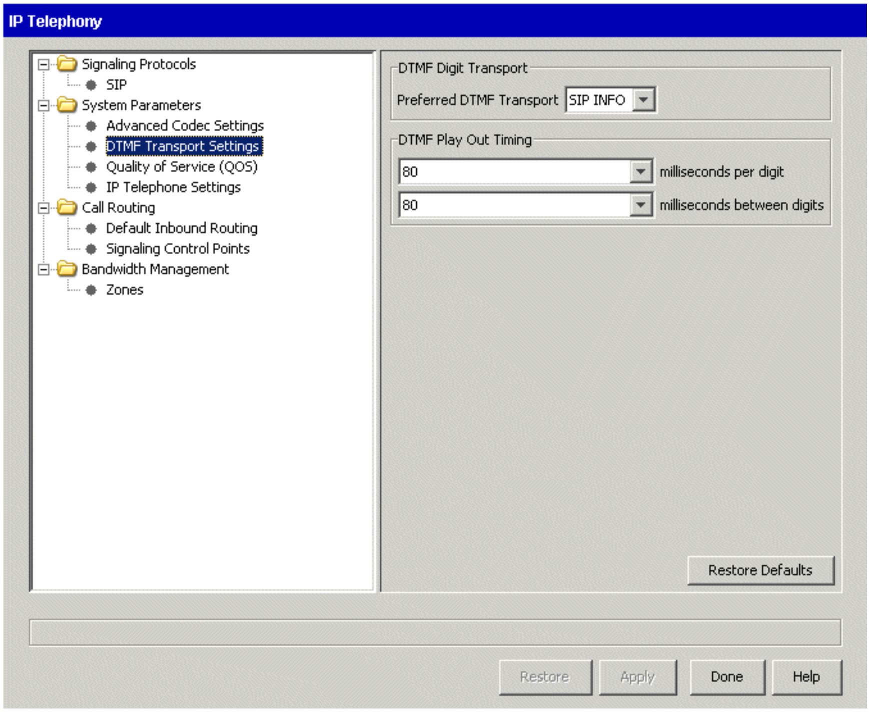
To configure the DTMF transport settings

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 In the left pane, expand System Parameters and then click **DTMF Transport Settings**.



Preferred DTMF Transport: SIP INFO

80 milliseconds per digit

80 milliseconds between digits

4 In the DTMF Digit Transport section, select one of the following from the **Preferred DTMF Transport** drop-down list, based on the requirements of your ITSP or SIP trunk provider.

- **Inband** (DTMF digits are left as tones in the original audio stream)
- **RFC 2833**
- **SIP INFO**

Note: This setting indicates a preference only - most ITSPs and SIP trunk providers use or prefer RFC 2833. If RFC 2833 is used by your ITSP or SIP trunk provider, Wave will automatically use RFC 2833, no matter what you specify here. On the other hand, if RFC 2833 is not supported by your ITSP or SIP trunk provider, Wave will use the setting that you specify.

5 In the DTMF Play Out Timing section, specify the following play out times in milliseconds:

- ___ **millisconds per digit**. Length of time that each DTMF digit plays.
- ___ **milliseconds between digits**. Length of time between each DTMF digit.

6 Click **OK**.

Quality Of Service (QoS) settings

Caution! *These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

Note: At least one Media Resource Module (MRM) is required on the Wave Server if you plan to use Quality of Service (QoS) settings with IP resources for VoIP calls. Contact your Wave provider for more information.

To configure the Quality of Service (QoS) settings

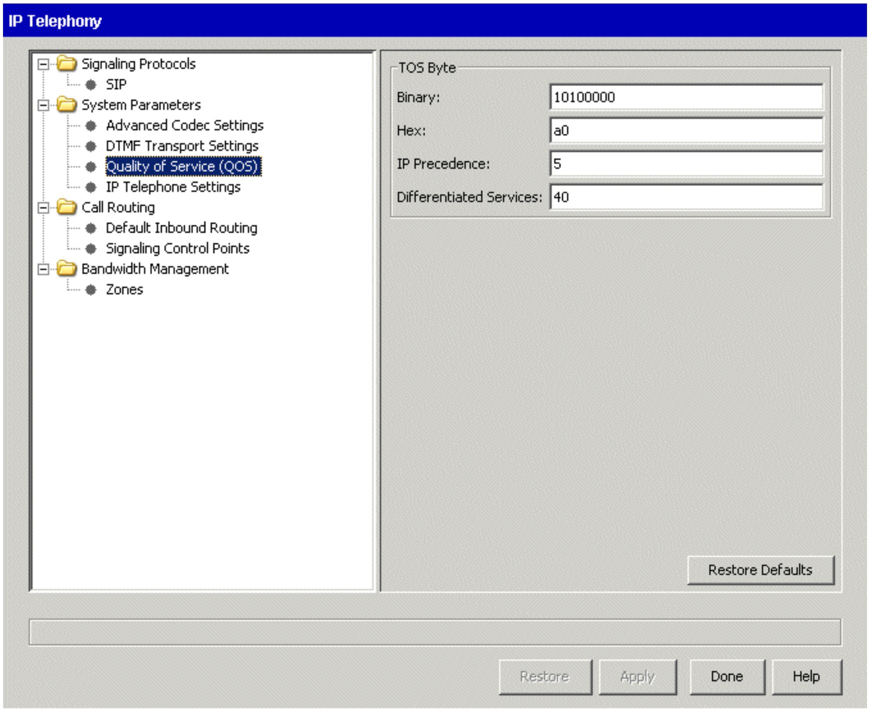
1 If necessary, click the Administration tab of the Management Console.

Click

IP

2 Click the IP Telephony icon, located in the PBX Administration section.

3 In the left pane, expand System Parameters and then click **Quality of Service (QOS)**.



IP Telephony

TOS Byte
Binary: 10100000
Hex: a0
IP Precedence: 5
Differentiated Services: 40

4 In the **TOS Byte** section, specify a value for one of the parameters. Changing the value in any of these fields adjusts the other fields to display equivalent values.

Note: Make a note of these values if you are connecting the Wave Server to an external router because you will need to specify these values when you configure prioritization of voice frames in the router.

5 Click **OK**.

Configuring Wave OpenVPN Server

Wave OpenVPN Server is the preferred method to enhance remote phone integration. (Another method is NAT traversal, described in “Configuring NAT traversal” on page 6-64.)

OpenVPN Server allows phones outside of your network to behave the same as local phones. With OpenVPN Server, when a remote user goes off-hook, the user’s phone automatically connects to your network. The OpenVPN Server extends your private network and its resources to support remote users with all the functionality and security available to local users.

OpenVPN Server is supported on the following Wave Gigabit-E SIP phones, which include a built-in virtual private network client. This client uses the OpenVPN protocol to support a secure connection to the Wave Server.

- Vertical IP Edge 5000i-LLCDG large LCD screen phone
- Vertical IP Edge 5000i-24G 24-button phone

Important! Before performing the steps in this section, see the *Wave OpenVPN Server Guide* for important information including application server, network, and VPN configuration requirements. That manual also provides detailed steps to download, install, and configure VMware vSphere Hypervisor™, a free platform for running a virtual machine on an application server, as well as required certificate generation and network routing configuration steps.

Be sure to perform all of the configuration steps described in Chapter 2 in the *Wave OpenVPN Server Guide* before configuring OpenVPN Server on your Wave Server as described in this section. You will need the following information from those steps:

- The Public IP address of the router or firewall that you port-forwarded
- The location where you saved the CA.crt file

You also need to set up OpenVPN Server for each user, and configure each user's SIP phone. See Chapter 3 in the *Wave OpenVPN Server Guide* for details.

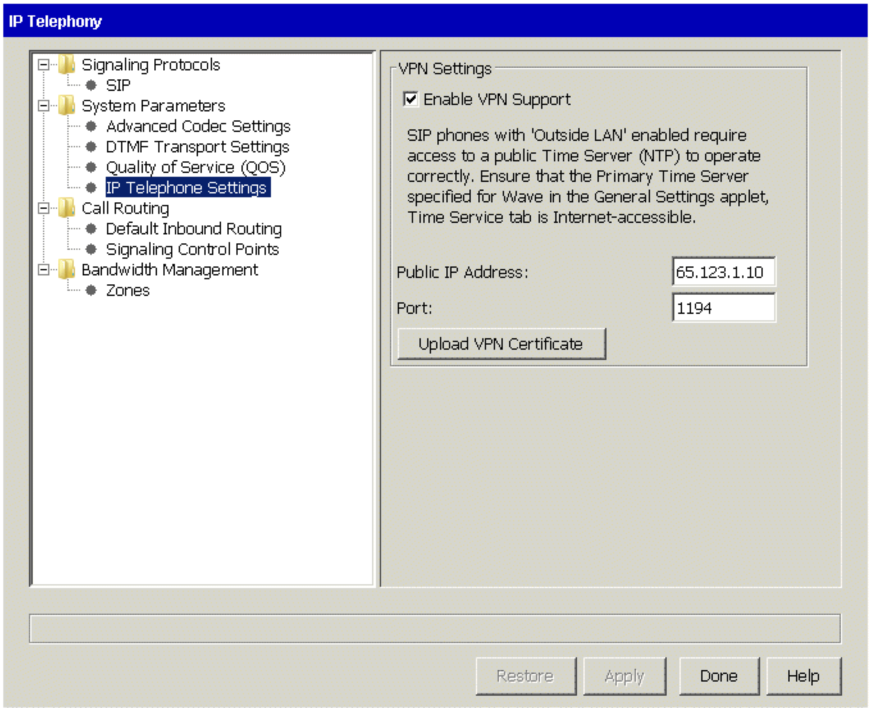
To configure OpenVPN Server

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 In the left pane, expand System Parameters and then click **IP Telephone Settings**.



IP Telephony

- Signaling Protocols
  - SIP
- System Parameters
  - Advanced Codec Settings
  - DTMF Transport Settings
  - Quality of Service (QOS)
  - IP Telephone Settings
- Call Routing
  - Default Inbound Routing
  - Signaling Control Points
- Bandwidth Management
  - Zones

VPN Settings

☑ Enable VPN Support

SIP phones with 'Outside LAN' enabled require access to a public Time Server (NTP) to operate correctly. Ensure that the Primary Time Server specified for Wave in the General Settings applet, Time Service tab is Internet-accessible.

Public IP Address: 65.123.1.10

Port: 1194

4 Select the **Enable VPN Support** checkbox.

5 Enter the following information:

- **Public IP Address**. Enter the Public IP address of the router or firewall that you port-forwarded to previously.
- **Port**. Enter 1194.

6 Click **Upload VPN Certificate**. Browse to the location where you saved the CA.crt file when you copied it from OpenVPN Server. Select the CA.crt file, and then click **Upload Certificate File**.

7 Click **Done** to save your changes, and then exit IP Telephony.

Configuring NAT traversal

NAT traversal is one method to enhance remote phone integration. NAT traversal is less secure than Wave OpenVPN Server, the preferred method, but is supported on all Vertical Edge SIP phones. (For more about Wave OpenVPN Server, see “Configuring Wave OpenVPN Server” on page 6-61.)

NAT traversal is a way to establish and maintain IP connections that traverse network address translation (NAT) gateways. NAT provides automated translation of IP addresses between different networks. For example, a company might use private IP addresses on a LAN that are represented by a single IP address on the WAN side of their router.

Configuring NAT traversal consists of the following tasks in the following order:

- **Configuring the Wave Server**, including enabling NAT traversal, specifying the STUN servers to use, and configuring the SCP. These steps are described below.
- **Configuring remote users** for NAT traversal, described in “Setting up NAT traversal for a user” on page 6-37.
- **Configuring your router** for NAT traversal. NAT traversal has been tested with two industry-leading routers:
  - Dell Sonicwall TZ 215-series router
  - Cisco 881 ISR router

  Other routers may work successfully, but Vertical cannot provide configuration details for all brands.

  See *Configuring the SonicWALL TZ215 Router for NAT Traversal* or *Configuring the Cisco 881 Router for NAT Traversal* for detailed router configuration steps.

Enabling NAT traversal and specifying STUN servers to use

Session Traversal Utilities for NAT (STUN) is a public service that is used to aid a phone or phone system in properly routing signaling so a call is successful and audio is present. A STUN server allows NAT clients (for example (for example a Wave Server behind a firewall) to set up phone calls to a VoIP provider hosted outside of the local Wave network.

When you deploy NAT traversal, best practice is to specify more than one STUN server:

- At least one STUN server must be specified for auto discovery to work.
- Typically a minimum of two STUN servers are specified to provide some level of fault tolerance.
- You can specify up to 3 STUN Servers.

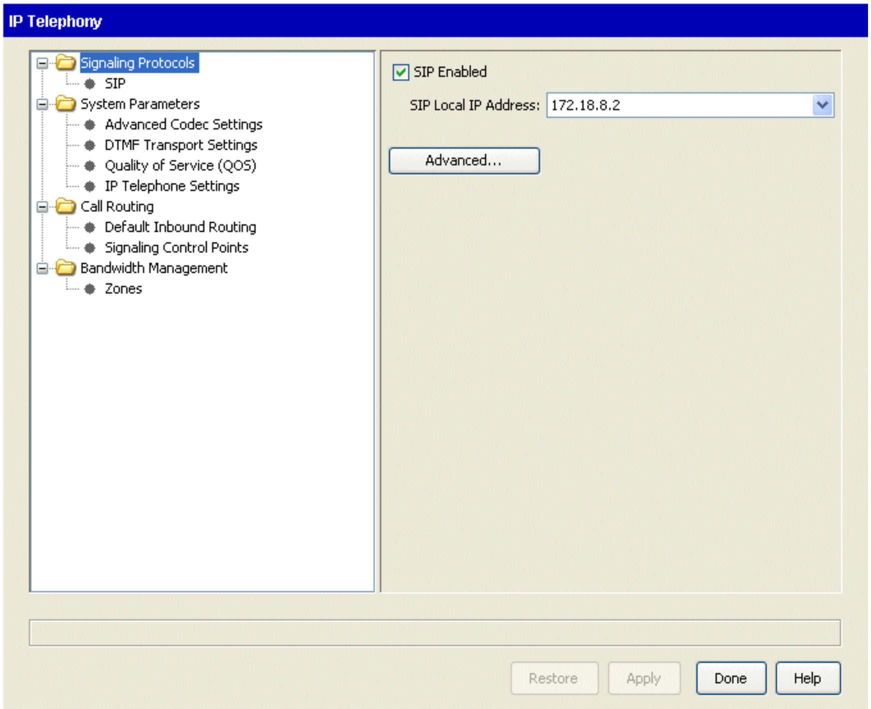
To enable NAT traversal and specify STUN servers

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 In the left pane, click **Signaling Protocols**, and then click **Advanced**.

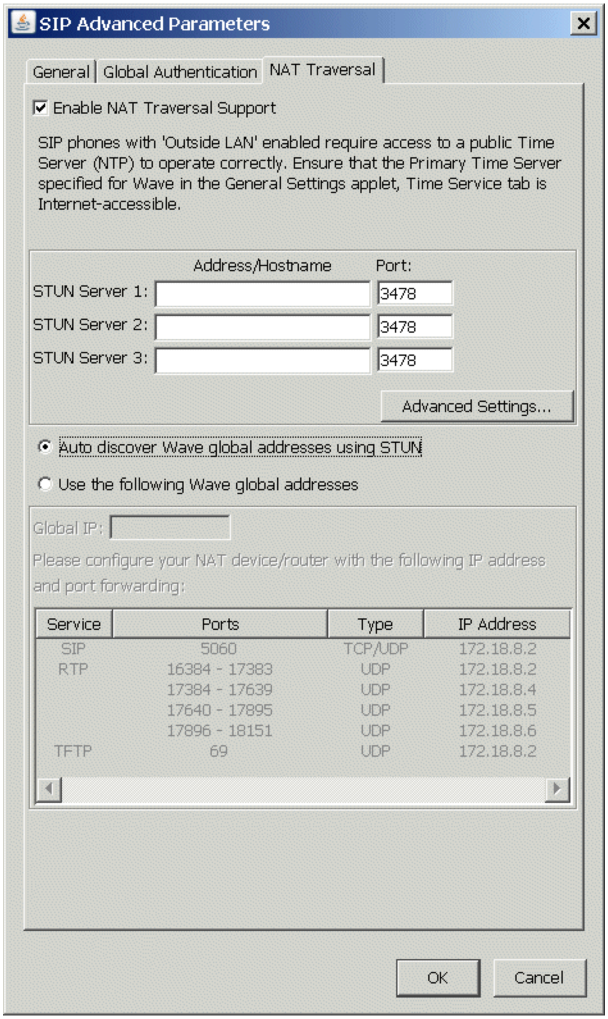


☑ SIP Enabled

SIP Local IP Address: 172.18.8.2

4 On the NAT Traversal tab, select the following options:

- **Enable NAT Traversal Support**
- **Auto discover Wave global addresses using STUN**



SIP Advanced Parameters

☑ Enable NAT Traversal Support

SIP phones with 'Outside LAN' enabled require access to a public Time Server (NTP) to operate correctly. Ensure that the Primary Time Server specified for Wave in the General Settings applet, Time Service tab is Internet-accessible.

	Address/Hostname	Port:
STUN Server 1:		3478
STUN Server 2:		3478
STUN Server 3:		3478

● Auto discover Wave global addresses using STUN

○ Use the following Wave global addresses

Global IP:

Please configure your NAT device/router with the following IP address and port forwarding:

Service	Ports	Type	IP Address
SIP	5060	TCP/UDP	172.18.8.2
RTP	16384 - 17383	UDP	172.18.8.2
	17384 - 17639	UDP	172.18.8.4
	17640 - 17895	UDP	172.18.8.5
	17896 - 18151	UDP	172.18.8.6
TFTP	69	UDP	172.18.8.2

You typically do not need to change the default STUN advanced settings.

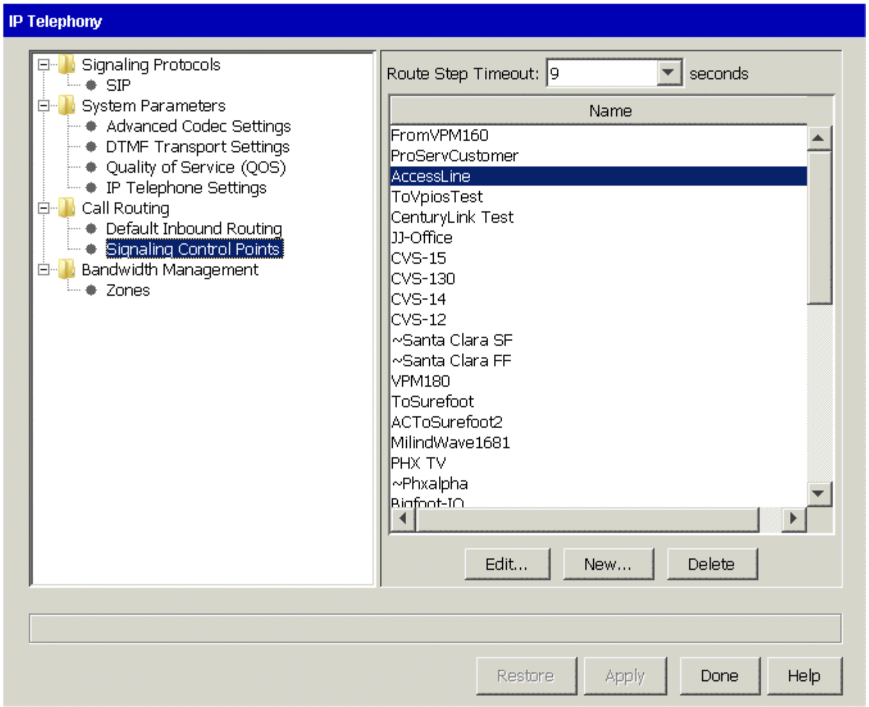
5 For **STUN Server 1**, **STUN Server 2**, and **STUN Server 3**, enter the IP address or hostname of each STUN server you are using.

Important! Note the table at the bottom of the SIP Advanced Parameters dialog on the previous page that lists the RTP port ranges and IP addresses used by each of the SIP endpoints on the Wave Server—the VAM and three MRM DSPs. You will use the IP address and port range information listed here when you configure your router for NAT traversal, as described in the configuration guide for your router. In this example, the four RTP services listed are for (in top-down order) the VAM, MRMA, MRMB, and MRMC.

6 Click **OK**.

To configure the SCP for NAT traversal

7 Expand **Call Routing** in the left pane, and then click **Signaling Control Points**.



IP Telephony

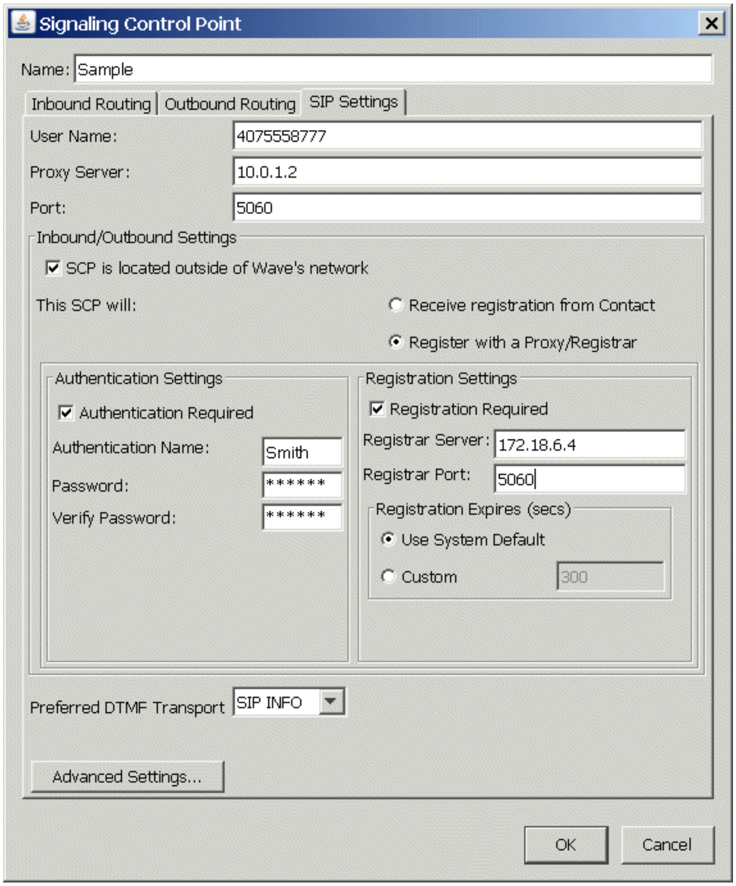
- Signaling Protocols
  - SIP
- System Parameters
  - Advanced Codec Settings
  - DTMF Transport Settings
  - Quality of Service (QOS)
  - IP Telephone Settings
- Call Routing
  - Default Inbound Routing
  - Signaling Control Points
- Bandwidth Management
  - Zones

Route Step Timeout: 9 seconds

Name
FromVPM160
ProServCustomer
AccessLine
ToVpiosTest
CenturyLink Test
JJ-Office
CVS-15
CVS-130
CVS-14
CVS-12
~Santa Clara SF
~Santa Clara FF
VPM180
ToSurefoot
ACToSurefoot2
MilindWave1681
PHX TV
~Phxalpha
Bigfoot-IO

8 Select your ITSP’s SCP and then click **Edit**.

9 Click the SIP Settings tab. In the Inbound/Outbound Settings section, select **SCP is located outside of Wave’s network**.



Signaling Control Point

Name: Sample

User Name: 4075558777

Proxy Server: 10.0.1.2

Port: 5060

Inbound/Outbound Settings

☑ SCP is located outside of Wave's network

This SCP will: ○ Receive registration from Contact ● Register with a Proxy/Registrar

Authentication Settings

☑ Authentication Required

Authentication Name: Smith

Password: ******

Verify Password: ******

Registration Settings

☑ Registration Required

Registrar Server: 172.18.6.4

Registrar Port: 5060

Registration Expires (secs)

● Use System Default

○ Custom 300

Preferred DTMF Transport SIP INFO

10 Click **OK**, and then exit IP Telephony.

How IP telephony ports are used

When using VoIP in a network, especially one that includes a firewall, you need to know the ports used by the packets that carry VoIP traffic. The following table lists these ports.

	Receive on...	**Transmit to...**
RTP Voice Transport		
RTP	UDP/dynamic (16384 - 18384) - not configurable	UDP/Dependant on other endpoint
RTCP	UDP/dynamic (16385 - 16835) - not configurable	UDP/Dependant on other endpoint
SIP Transport		
	5060 - configurable to 5061	5060, 5061
	UDP 65000 (used for music on hold)	

Chapter 7

Initial Call Routing Configuration

CHAPTER CONTENTS

This chapter provides information about configuring initial call routing options and internal call routing settings.

About the First Digit Table

First Digit Table settings are used to assign telephone dial pad numbers 0 to 9 to various call types--including internal, external, off-premise, and attendant--based on the call destination. The First Digit Table settings affect many other Wave settings for trunks, the PBX, extensions, AutoAttendant, and Voice Mail.

The First Digit table is preconfigured with the most commonly-used settings—9 for an external line, 0 for the company operator, and so forth. If the default first digit settings listed below are satisfactory, you do not need to reconfigure the First Digit Table applet

Caution! *Any changes you want to make to the first digit table defaults should be made before trunk and PBX configuration.*

FIRST DIGIT TABLE DEFAULT SETTINGS

First Digit	Default Setting	Use
0	**Attendant**	Instructs the PBX to connect to the system operator. The system operator extension is specified when you configure the Attendant hunt group via the Hunt Groups applet. (See “Configuring the Attendant hunt group” on page 10-44 for more information.)
1, 5	**Extension**	Instructs the PBX to connect calls beginning with these digits to an internal or off-premise extension of the length defined. Default user extensions begin with any digit in the range 100 through 199. You can create extensions that begin with any number from 1 to 9 and they can be up to 7 digits long. Default system-wide extensions, such as modems, begin with any digit in the range 500 through 599; for example, Wave Server modems are preconfigured to use extension 570. Like other Wave Server defaults, this can be changed. The default extension length is three, with a range of two to seven.
2, 3, 4, 6, 7, 8	**Not configured**	Instructs the PBX that calls beginning with these digits are not valid. If a user dials a first digit that has not been configured, the PBX plays a “fast busy” signal immediately to indicate that the first digit dialed is invalid. All of these first digits can be configured to be used for extension or external settings.
9	**External**	Instructs the PBX that an outbound, external call (to be routed through the Central Office) is beginning. For example, the default 9 requires all users to press 9 on their telephone dial pad before dialing any number outside the building on the public switched telephone network (PSTN). You can change the External access code to any number between 1 and 9 You can define the external first digits (access codes) as being one or two digits in length. The default is one digit. If you select the external dialing to require two digits, then you can configure the digits 90 through 99. For each access code you can select the type of routing, configured in the Outbound Routing applet, the number of digits to collect after the access code, and whether or not to provide dial tone after that particular access code is dialed.

You use the First Digit Table applet to do the following:

- Configure extension ranges. See page 7-3.
- Set the home area code. See page 7-5.
- Configure 10-digit dialing. See page 7-6.
- Configure the external first digit for outbound call routing. See page 9-2.

You use the User/Group Management applet to configure the VoiceMail extension. See page 7-7.

Configuring extension ranges

In this task you will configure the digits extensions can begin with, and the number of digits in extension numbers.

The default ranges for extensions are as follows:

- User extensions are 100-199 (first digit 1, length 3)
- System extensions are 500-599 (first digit 5, length 3)

  For example, Wave Server modems are preconfigured to use extension 570.

Note: If you have already configured extensions, and you want to change the extension length, you must first delete all the extensions, hunt groups, and voice mailboxes that begin with the first digit in the range you want to modify.

To configure extension ranges

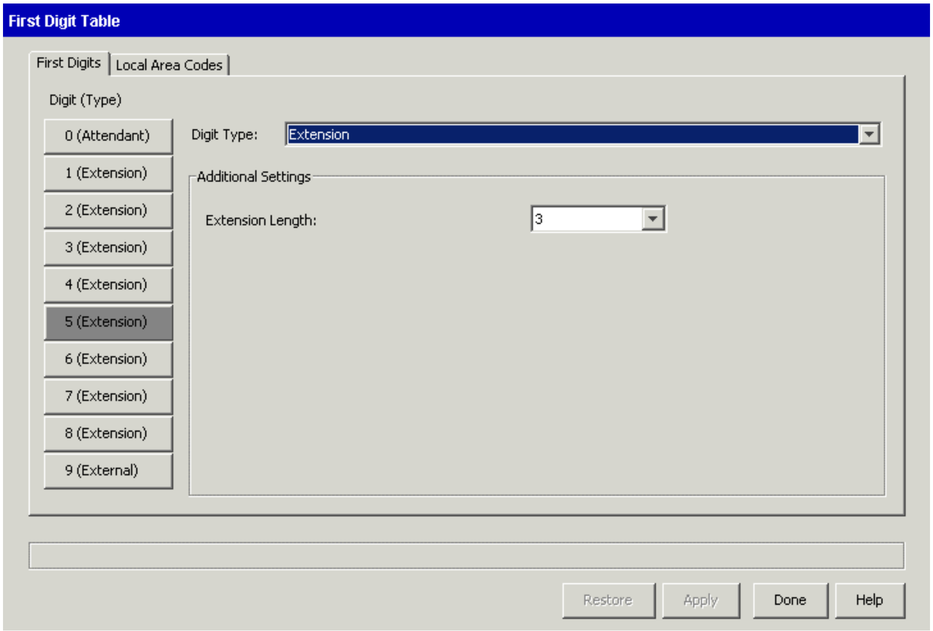
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 The First Digit Table applet starts.

4 Select one of the **Digit (Type)** buttons from the left side of the applet, and then select **Extension** from the **Digit Type** drop-down list.



Digit Type: Extension

Extension Length: 3

5 Select an extension length between 2 and 7 digits from the **Extension Length** drop-down list. For example, selecting Digit 1 with an extension length of 3 will provide you with extension numbers in the range 100-199.

6 Click **Apply** to save your changes.

7 Click **Done** to return to the Management Console.

Setting the home area code

When the user dials a seven-digit local telephone number, automatic route selection uses the home area code to find a matching rule in the area code tables.

Note: If you change the Wave Server system locale setting (as described in Setting and viewing system locale settings), you may need to update existing area codes to reflect the lengths allowed for the new locale.

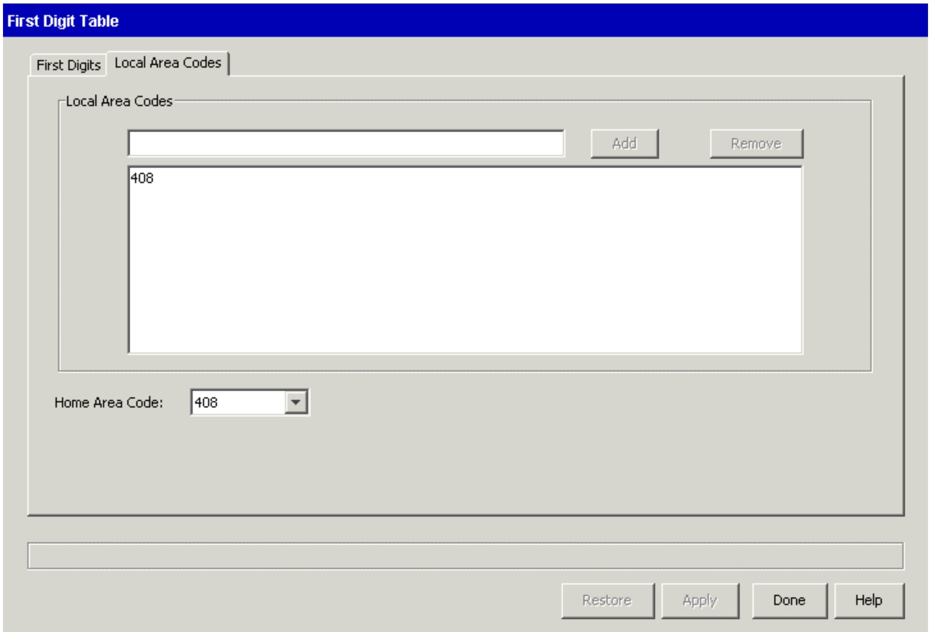
To specify your home area code

1 If necessary, click the Administration tab of the Management Console.

2 Click the First Digit Table icon, located in the PBX Administration section.

Click

3 Click the Local Area Codes tab.



First Digit Table

First Digits | Local Area Codes

Local Area Codes

408

Home Area Code: 408

4 Enter your home area code in the **Local Area Codes** text box, and then click **Add**.

The area code is displayed in the list below the field.

Do not specify any additional area codes unless your calling area requires 10-digit dialing for local area codes. See “Configuring 10-digit dialing” on page 7-6.

The area code that you enter is also displayed in the **Home Area Code** drop-down list.

5 Select your **Home Area Code** from the drop down list.

6 Click **Apply** to save your changes.

7 Click **Done** to the Management Console.

Configuring 10-digit dialing

Configure 10-digit dialing when certain telephone numbers that include the area code do not require that a 1 be dialed before dialing the telephone number.

To configure 10-digit dialing

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 Click the Local Area Codes tab.

4 Enter each area code in the **Local Area Codes** text box, and click **Add** to add it to the list.

Note: If you must dial a 1 before using an area code, do not enter that area code in the **Local Area Codes** list.

Note: Be sure that your home area code is selected in the **Home Area Code** drop-down list.

5 Click **Apply** to save your changes.

6 Click **Done** to return to the Management Console.

Note: In some cases you might want to have users dial ten digits but your service provider requires 11 digits for calls to specific area codes. You will need to add a 1 to the number before placing the call. To configure this digit manipulation, see “Configuring outbound routing tables” on page 9-20.

Configuring the VoiceMail extension

The VoiceMail default extension (550) is adequate for most Wave configurations, If you want to use a different extension number to access voicemail, perform the following steps.

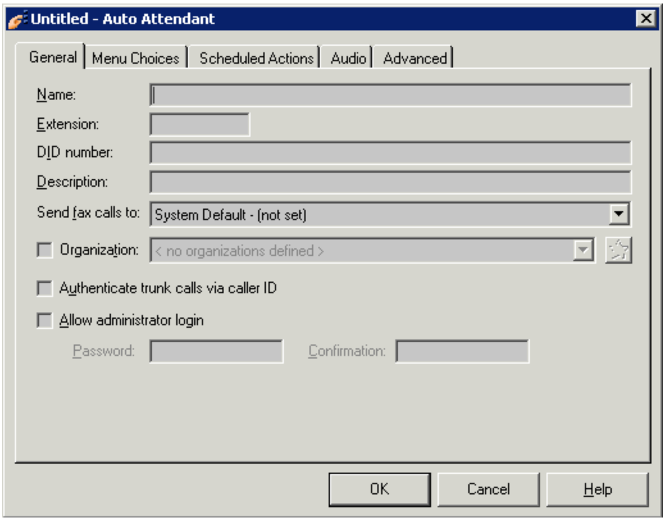
To configure the VoiceMail extension

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section.

3 Click **File > New > Auto Attendant**.



Name:
Extension:
DID number:
Description:
Send fax calls to: System Default - (not set)
□ Organization: < no organizations defined >
□ Authenticate trunk calls via caller ID
□ Allow administrator login
Password: Confirmation:

4 Enter the following information on the General tab:

- **Name**. Required. Descriptive name for the new auto attendant, for example, “VoiceMail”.
- **Extension**. Required. Extension used to access VoiceMail.

5 Click **OK** to close the Auto Attendant dialog.

6 Click **Done** to return to the Management Console.

Click

7 Click the General Settings icon, located in the General Administration section.

8 In the General Settings dialog, click the System tab and then select the newly-created auto attendant from the **Voice Mail System** drop-down list.

9 Click **Apply** to save your changes.

10 Click **Done** to return to the Management Console.

Chapter 8

Configuring Inbound Call Routing

CHAPTER CONTENTS

This chapter describes how to configure the Wave Server for inbound call routing.

For inbound call routing configuration recommendations and examples, see “Inbound call routing” on page 29-16.

Configuring trunk groups for inbound call routing

You created trunk groups, and configured the outbound trunk hunt order in “About creating new trunk groups” on page 5-2.

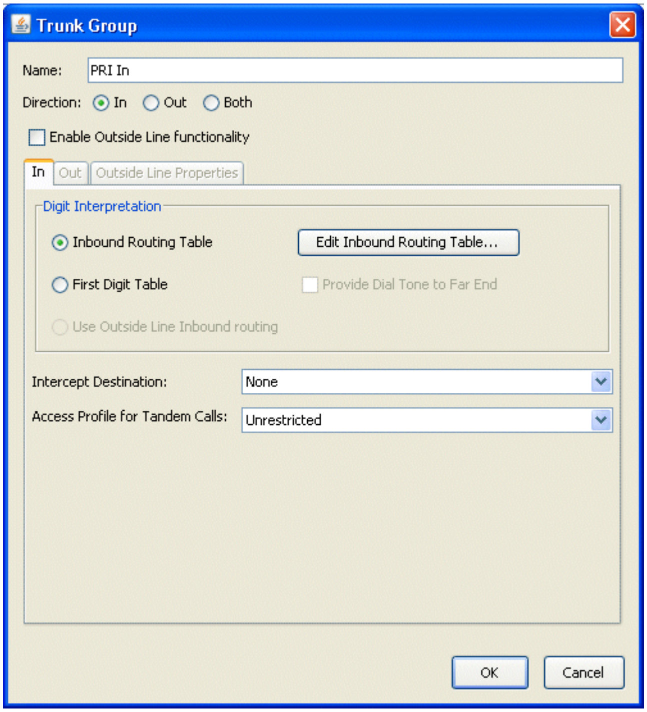
To configure trunk groups for inbound call routing

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Groups icon, located in the Trunk Administration section.

3 Select and edit a trunk group for inbound call traffic. The Trunk Group dialog opens.



Trunk Group

Name: PRI In

Direction: ● In ○ Out ○ Both

□ Enable Outside Line functionality

Digit Interpretation

● Inbound Routing Table

○ First Digit Table

□ Provide Dial Tone to Far End

○ Use Outside Line Inbound routing

Intercept Destination: None

Access Profile for Tandem Calls: Unrestricted

4 On the In tab, specify how to interpret received digits from an inbound call:

- **Inbound Routing Table**. Select this option if Wave will be receiving calls from a central office switch. If you choose this option, refer to “Configuring inbound routing tables” on page 8-4, for detailed instructions about setting up your inbound routing tables. Click **Edit Inbound Routing Table** to make changes to the table.
- **First Digit Table.** Select this option if Wave will be receiving calls from another PBX, rather than from a central office switch. Refer to “Configuring extension ranges” on page 7-3, for detailed instructions about setting up the First Digit Table.

  Check the **Provide Dial Tone** check box if Wave must provide dial tone to the far end.
- **Use Outside Line Inbound Routing.** This field is only enabled if this is an outside line-enabled trunk group. If this option is selected, inbound calls to associated digital phones will be terminated with no digit manipulation. See Chapter 5 for more about creating outside line-enabled trunk groups.

5. In the **Intercept Destination** field, enter the extension or hunt group to which you want to send calls that cannot be routed using Inbound Routing Table rules. All calls received on this inbound trunk group that fail for any reason will be sent to the station or hunt group that you specify. Examples of failed calls are a misdialed number or an external number that is blocked by this trunk group's tandem access profile.

   Note: If you select **None**, callers who cannot be routed simply hear a fast-busy tone.

   Caution! *Do not configure the Wave Server to route inbound calls to the Intercept Destination by default. This might cause your calls to be routed incorrectly. If you would like to create a true inbound call default destination, create a default step in the inbound routing table.*

6. Select **None** if your call routing does not provide for tandem (or trunk-to-trunk) calls, and go to step 7.

   Important! This step only applies if you have configured the Wave Server for tandem call routing.

   To restrict the use of the Wave Server in a tandem call routing configuration to prevent toll fraud, select the **Access Profile for Tandem Calls** from the drop-down list. (For information about tandem calls, see "Tandem call routing" on page 29-22.)

   Click

   If you configure the Wave Server to handle tandem calls, you must also select the **Allow External Trunk-to-Trunk Connections** option in the General Settings applet, PBX (Advanced) tab, Trunking group box. In this scenario, a call is physically connected across two external trunks through the Wave Server. If you enable external trunk-to-trunk connections, the Wave Server allows calls to be forwarded, transferred, and conferenced between external numbers.

   Note: Trunk-to-trunk connections involving analog loop-start trunks are not included in this option by default because such connections may not terminate properly even when a call is completed, resulting in a trunk remaining unavailable even when it is not actively being used. It is recommended that you accept this default.

Note: If your particular needs require that users be able to make analog loop-start external trunk-to-trunk connections, make the following additional settings in the Trunking group box:

- Select the **Allow Analog Loop-Start Trunk-to-Trunk Connections** option.
- Choose a maximum duration for trunk-to-trunk connections from the **Trunk-to-Trunk Maximum Connect Time (Minutes)** drop-down list. This setting limits the amount of time a trunk may be unavailable when not actively being used, but it also determines the maximum duration of active calls. Be sure to choose a setting that won’t result in active calls being cut off prematurely.

7 Click **OK** to save your changes.

Configuring inbound routing tables

For information about and examples of inbound routing tables, see “Inbound call routing” on page 29-16.

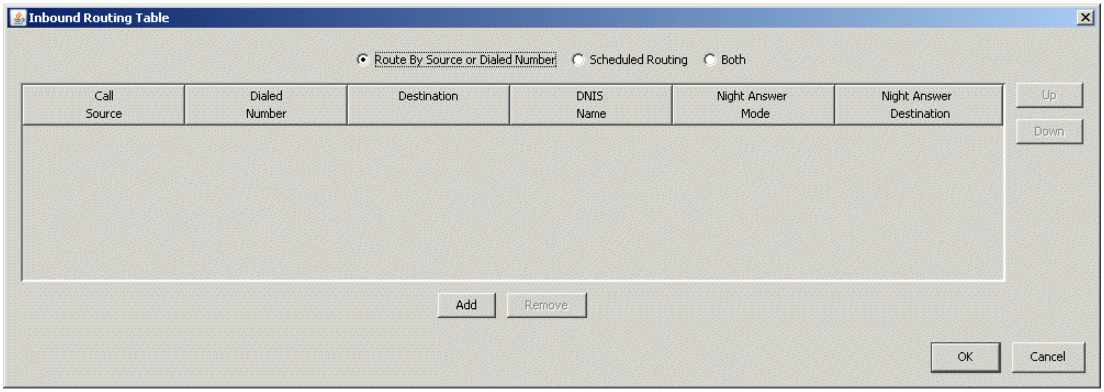
To configure an inbound routing table

1 If necessary, click the Administration tab of the Management Console.

2 Do one of the following:

- Click the Trunk Groups icon, located in the Trunk Administration section. On the In tab, click **Edit Inbound Routing Table**.
- Click the IP Telephony icon, located in the PBX Administration section. Select the Call Routing folder, and then click **Edit Inbound Routing Table**.

The Inbound Routing Table dialog opens.



Inbound Routing Table

● Route By Source or Dialed Number ○ Scheduled Routing ○ Both

Call Source	Dialed Number	Destination	DNIS Name	Night Answer Mode	Night Answer Destination

3 Select one of the following routing methods for the routing rules in the inbound routing table.

Warning: *It is generally recommended that you use the "Both" method all the time. This is because any routing rules entered and saved in the inbound routing table will be lost if you change to another routing method at a later time. (For example, if you initially set up the inbound routing table rules using the “Route By Source” method and then want to change to use “Scheduled Routing” , the data in the routing table will be deleted when the new method is selected.) When you select "Both" when you set up your inbound routing table rules, you have access to all routing method fields available when you choose either of the other methods, and you do not run the risk of having to re-enter all of your routing rules if they get deleted when you change methods.*

- **Route By Source or Dialed Number.** Using this setting you can decide how calls on this trunk group get routed based on the Caller ID (or ANI) sent with the call, or the digits the caller dialed (DID, Lead Telephone Number, or DNIS).
- **Scheduled Routing**. Use this format to set time and day restraints on the destination to which inbound calls from the specified trunk are routed. This choice is ideal for trunks that receive no digits and require no translation.
- **Both**. This setting is ideal if calls to the main company number and all numbers are sent to the same trunk group. This setting also gives you access to all routing method fields available when you choose **Route By Source or Dialed Number** or **Scheduled Routing**.

4 Click **Add** to insert a new rule into the table.

- If you selected **Scheduled Routing** in step 3:
    - Select the checkboxes for any days of the week when you want this rule to be applied.
    - Select times in the **Start Time** and **End Time** fields during which you want this rule to be applied.
- If you selected **Route By Source or Dialed Number** in step 3, click the appropriate table cells to enter values in the following columns:
    - **Call Source**. No value required. May be any string of digits representing Caller ID or ANI source number.
    - **Dialed Number**. “Default” (wildcard value, indicating that any number received, of any length, is accepted.), or contains a string of zero or more digits, followed by a string of 0 or more x characters. This string may be as large as 32 characters. The dialed number column directly represents the digits expected to be sent from the CO with an inbound call. For example, enter a three-digit number beginning with a 2 as the value 2xx.
- If you selected **Both** in step 3, you can create a rule using any of the fields described for the other 2 methods.

5 Enter the destination information.

- **Destination**. Contains a string of zero or more digits, followed by a string of 0 or more x's. This string may be as large as 32 characters. This number is interpreted as if dialed from an internal station. For example, enter a three-digit extension number beginning with a 1, as the value 1xx. If the destination is an external telephone number, append the external access digit (configured in the First Digit Table) before the telephone number.
- **DNIS Name**. No value required. If the value in the Dialed Number field is a DNIS number, enter a description up to 32 characters long. This description overwrites the calling party (call source) information and is displayed on the display panel of the destination extension. This string identifies the number that the caller dialed.

6 Enter one of the following **Night Answer** modes from the drop-down list.

- **Not Used**. Disables the Night Answer Mode
- **Use System Default**. Uses the **Default Night Answer Destination** specified in the General Settings applet
- **User Defined**. Uses the destination that you enter in the Night Answer Destination field and overrides the system default specified in the General Settings applet

7 Select a rule, and click **Up** and **Down** to rearrange the rule order.

If you selected **Scheduled Routing** in step 3 and there is overlap in the schedule, the rules must appear in order of precedence.

8 Click **OK** to return to the host applet.

9 Click **Apply** to save your changes.

10 Click **Done** to return to the Management Console.

Chapter 9

Configuring Outbound Call Routing

CHAPTER CONTENTS

Outbound call routing determines how calls that originate within Wave Server and that terminate at an external destination are handled.

See "Outbound call routing" on page 29-4 for background information on the types of outbound call routing described in this chapter.

Configuring automatic route selection

This section provides information about configuring outbound call routing using automatic route selection. See "Automatic route selection" on page 29-8 for examples and information about why you might use automatic route selection. To set up your Wave Server for automatic route selection, you need to complete the following tasks:

- Configuring the external first digit. See page 9-2.
- Configuring the Global Access Profile. See page 9-4.
- Configuring specific access profiles. See page 9-14.
- Configuring outbound routing tables. See page 9-20.

Configuring the external first digit

In this task you will configure an external first digit for outbound call routing by automatic route selection.

To configure the external first digit

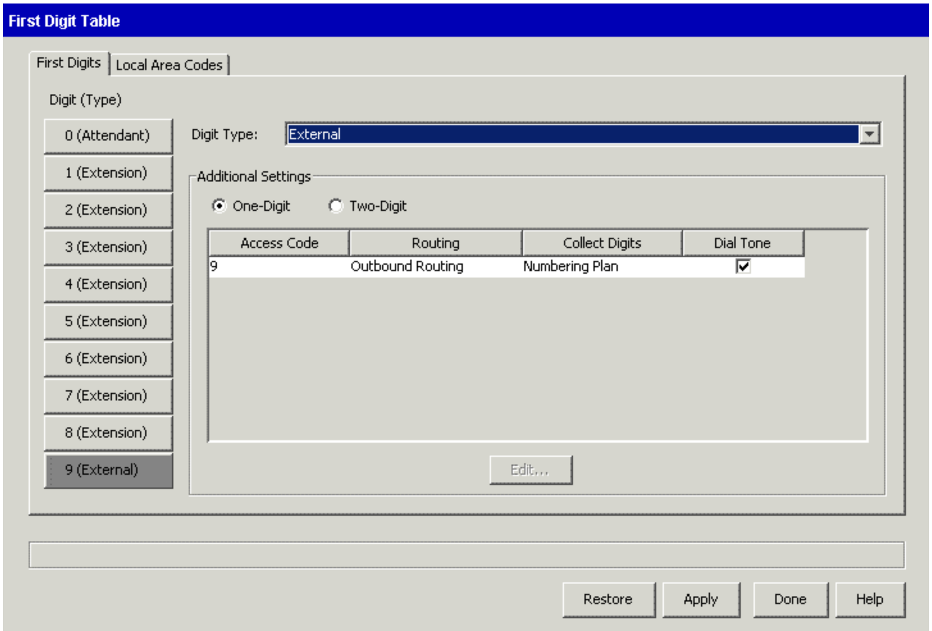
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 Select a **Digit (Type)** button and set **Digit Type** to **External**.

The external digit configuration options appear in the Additional Settings group box.



First Digit Table

First Digits | Local Area Codes

Digit (Type)

Digit Type: External

Additional Settings

● One-Digit ○ Two-Digit

Access Code	Routing	Collect Digits	Dial Tone
9	Outbound Routing	Numbering Plan	☑

4 Specify whether you want this first digit to support **One-Digit** or **Two-Digit** external dialing.

If you select Two-Digit external dialing, access codes *x*0 through *x*9 (where *x* is the first digit) appear in the Additional Settings table.

5 Check to make sure the settings for the access code (or for each access code, if Two-Digit support is selected) are as follows. If not, double-click the access code to display the Edit External Access Code dialog and make the necessary changes.

- **Routing**. Leave this option set to the default of **Outbound Routing**.
- **Collect Digits**. Leave this option set to the default of **Numbering Plan**.

  This setting automatically selects the numbering plan for your locale. For North America this is the North American Numbering Plan (NANP).
- **Dial Tone**. If you want Wave to provide a dial tone when the external digit or digits are dialed, leave the **Dial Tone** check box selected. If not, deselect the check box.

6 Click **Apply** to save your changes.

7 Click **Done** to return to the Management Console.

Configuring how first digit extensions appear in ViewPoint

You can give an external first digit a name, to make it easier for users to select in ViewPoint. You can also hide an external first digit so that it does not appear in ViewPoint and cannot be dialed. Hiding first digits can be useful when you want to use them for testing purposes.

To configure an external first digit for ViewPoint

1 If necessary, click the Administration tab of the Management Console.

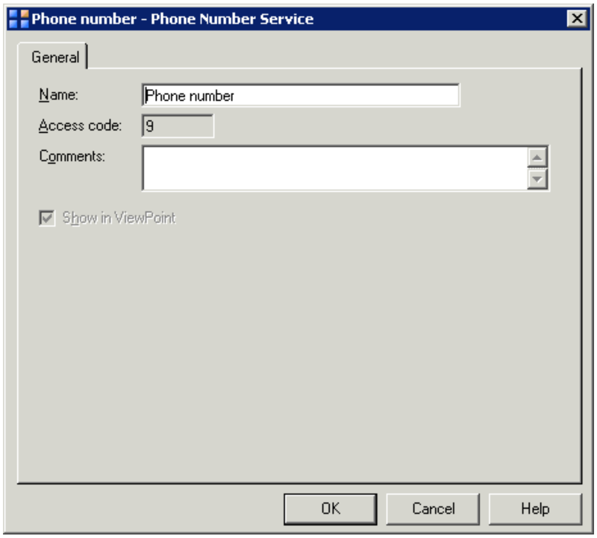
Click

2 Click the User/Group Management icon, located in the PBX Administration section. The User/Group Management applet opens.

See “Using the User/Group Management applet” on page 2-15 for information about navigating in the User/Group Management applet.

3 Click the Dialing Services icon in the view bar. The Dialing Services view opens, displaying all external first digits that you have defined so far.

4 To edit a dialing service, double-click it in the view. The Dialing Service dialog opens.



Name: Phone number
Access code: 9
Comments:
☑ Show in ViewPoint

5 Type the dialing service **Name**.

6 Add any notes about the dialing service in **Comments**.

7 Select the **Show in ViewPoint** checkbox if you want this dialing service to be available for use in all **Call Using** lists in ViewPoint.

8 Click **OK**.

Configuring the Global Access Profile

Wave examines the Global Access Profile settings prior to examining the specific access profile for an outbound call.

Note: To support automatic dialing from ViewPoint over analog phone lines, you must reconfigure the Global Access Profile. For instructions, see “Configuring the Area Code table for ViewPoint analog dialing” on page 9-13.

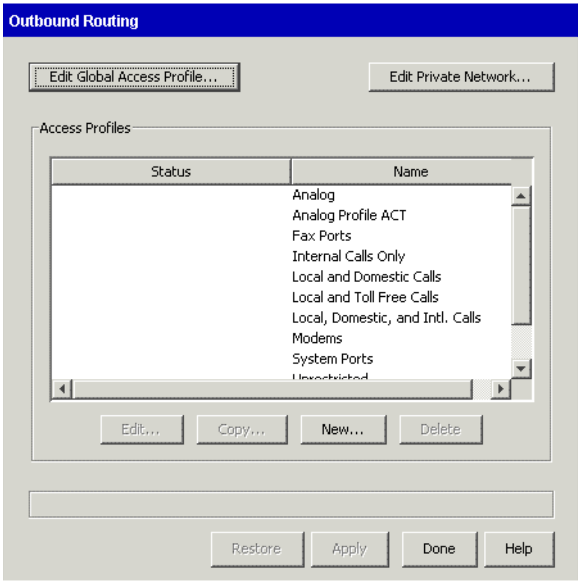
To edit the Global Access Profile

Click

1 If necessary, click the Administration tab of the Management Console.

2 Click the Outbound Routing icon, located in the Trunk Administration section.

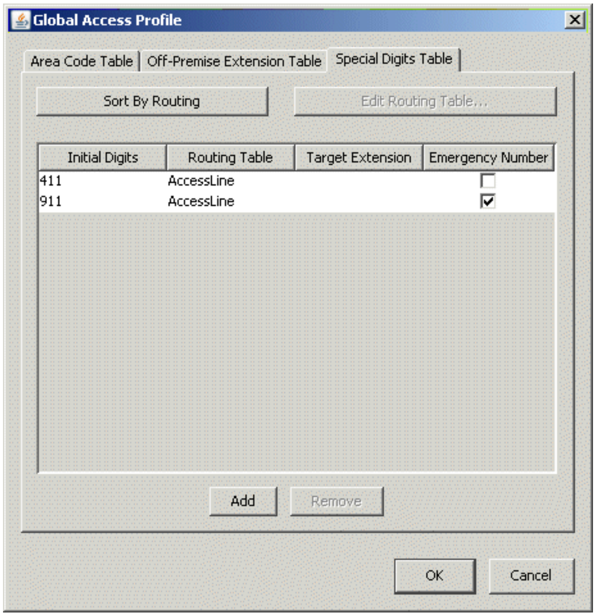
3 The Outbound Routing dialog opens:



Status	Name
	Analog
	Analog Profile ACT
	Fax Ports
	Internal Calls Only
	Local and Domestic Calls
	Local and Toll Free Calls
	Local, Domestic, and Intl. Calls
	Modems
	System Ports
	Unrestricted

4 Click **Edit Global Access Profile** to open the Global Access Profile dialog.

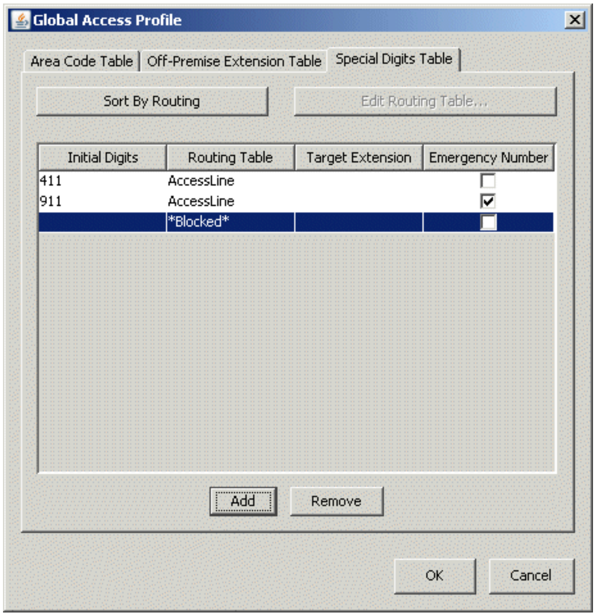
5 Click the Special Digits Table tab. You use the Special Digits Table to enter any digits or strings of digits that you want Wave to process before processing the rules in the other tables.



Initial Digits	Routing Table	Target Extension	Emergency Number
411	AccessLine		□
911	AccessLine		☑

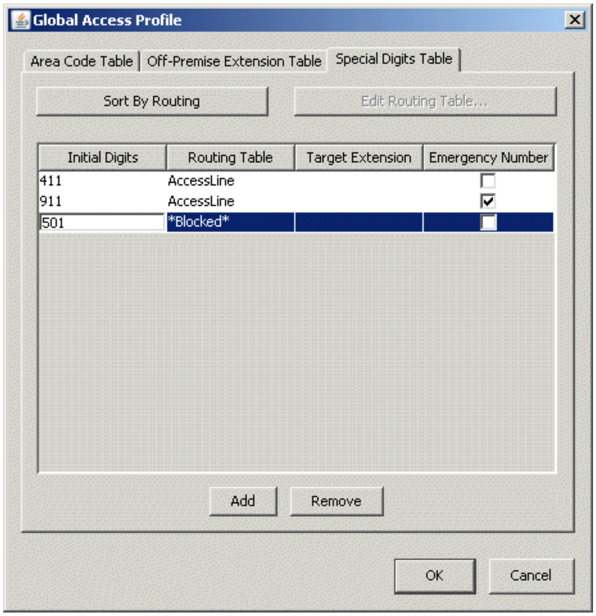
Note: The default emergency number for your locale (911 for North American systems and 112 for EU systems) is automatically configured as a special digit string and is routed to the Voice Analog routing table. For more about setting up emergency dialing via the Outbound Routing applet, see “Setting up emergency dialing” on page 9-43.

6 Click **Add** to add a new special digit string. A new row is added to the table.



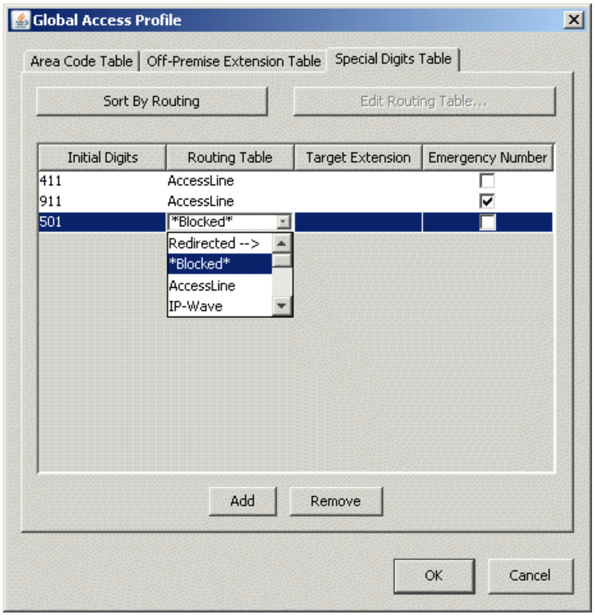
Initial Digits	Routing Table	Target Extension	Emergency Number
411	AccessLine		☐
911	AccessLine		☑
	Blocked		☐

7 Double-click in the **Initial Digits** column in the new row to open a text box, and then enter the special digit string.



Initial Digits	Routing Table	Target Extension	Emergency Number
411	AccessLine		□
911	AccessLine		☑
501	*Blocked*		□

8 To specify how to handle calls that start with this special digit string, click in the **Routing Table** column to open a drop-down list.



Initial Digits	Routing Table	Target Extension	Emergency Number
411	AccessLine		☐
911	AccessLine		☑
501	*Blocked*		☐

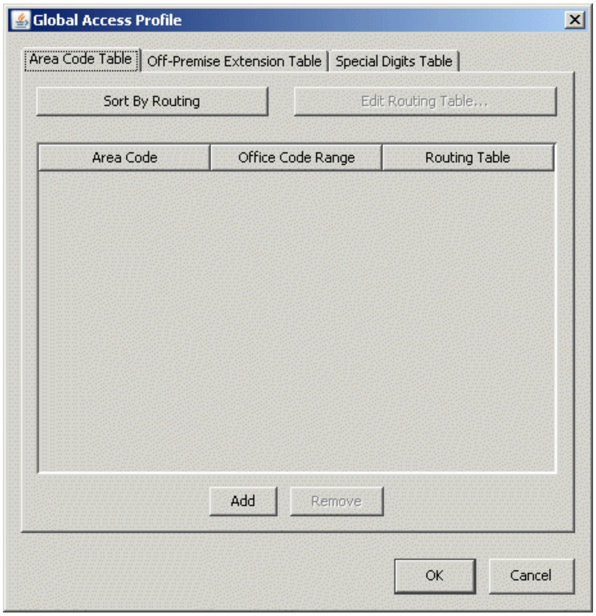
Select one of the following options from the drop-down list:

- A routing table that has already been defined. Calls that start with this special digit string will be handled by the routing table that you select.
- **Redirected -->**. Select this option to redirect calls that start with this special digit string to another extension.
- ***Blocked***. Select this option to block all calls that start with this special digit string.
- **(New Routing Table)**. Select this option to create a new routing table to handle calls that start with this special digit string. See “Configuring outbound routing tables” on page 9-20 for instructions.

9 If you selected **Redirected -->** in the previous step, click in the **Target Extension** column to open a drop-down list, and then select the extension to which you want to redirect the call.

10 Click **Sort By Routing** to arrange the rules in the order they should be applied during outbound call routing.

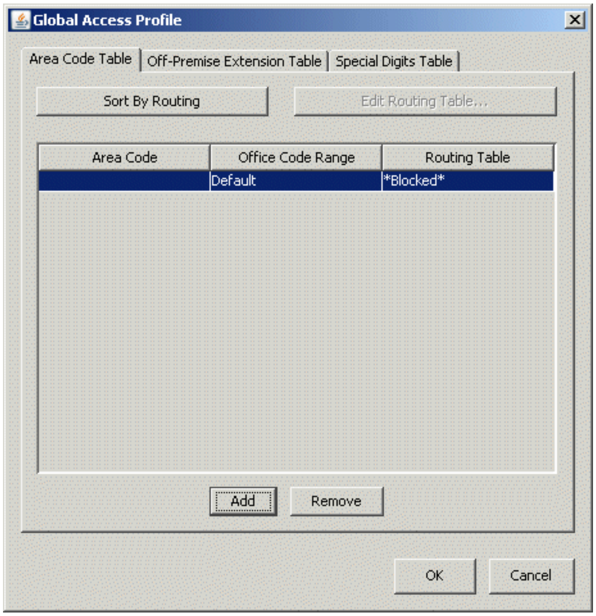
11 Select the Area Code Table tab.



The Area Code Table is where Wave looks for matching area codes or office codes (or combinations of area and office codes) to determine how to route calls containing those numbers. You can use the Global Access Profile Area Code Table to block undesirable toll calls.

The rules that you specify in the Global Access Profile Area Code Table override the rules that you set for the specific access profiles area code tables you will configure later in this section. If you want to block or route certain numbers for all users in the system, enter the rules in this table.

12 Click **Add** to add an entry to the Area Code Table. A new row is added to the list.

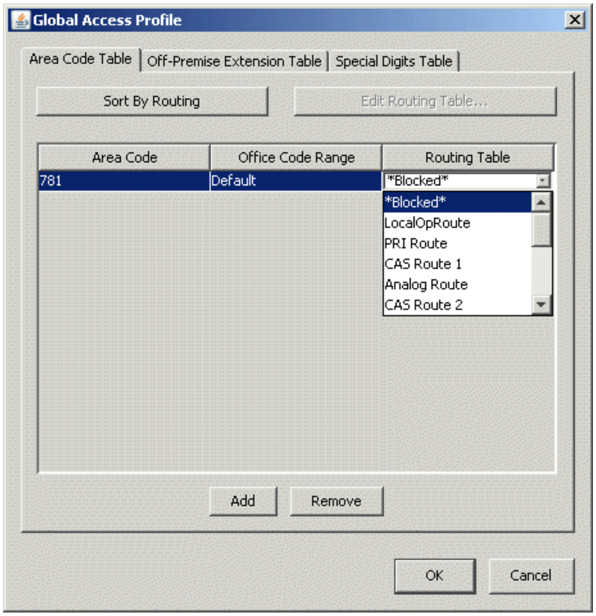


Area Code	Office Code Range	Routing Table
	Default	*Blocked*

13 To enter the **Area Code** and **Office Code Range** for the new area code, double-click in each column in the new row, and then enter the codes for which you are providing routing instructions.

- **Area Code**. Enter the area code for which you want to specify routing instructions that apply to all outgoing calls. You might want to add an entry to block outbound calls with an area code of 900. Enter **Default** to allow all area codes.
- **Office Code Range**. Enter the office code (or a range of office codes) within the specified area code. Enter **Default** to match any office code within the specified area code.

14 Click in the **Routing Table** column to open a drop-down list.



Area Code	Office Code Range	Routing Table
781	Default	*Blocked*

Select one of the following options from the drop-down list:

- A routing table that has already been defined. Calls to this area code will be handled by the routing table that you select.
- ***Blocked***. Select this option to block all calls to this area code.
- **(New Routing Table)**. Select this option to create a new routing table to handle calls to this area code. See “Configuring outbound routing tables” on page 9-20 for instructions.

15 Repeat steps 12 through 14 to enter additional area code and office code routing entries.

16 Click **Sort By Routing** to arrange the rules in the order they should be applied during outbound call routing.

17 When you are finished editing the Global Access Profile, click **OK** and save your changes.

18 Click **Apply** to save your changes.

19 Click **Done** to return to the Global Administrator Management Console.

Configuring the Area Code table for ViewPoint analog dialing

You must configure Wave as follows to support automatic dialing from ViewPoint over analog lines.

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section. The Outbound Routing applet opens.

3 Click **Edit Global Access Profile**. The Global Access Profile dialog opens.

4 Click the Area Code Table tab if it is not already selected.

5 Add the following rules to the Area Code Table:

- To add support for 11-digit dialing for specific exchanges, add a new entry in the area code table, enter the area code and a range of Office Codes (exchanges), then create a new routing table and specify to keep the last 7 digits and to prepend 1+XXX where XXX is the area code.
- To add support for 10-digit dialing for specific exchanges, add another entry in the area code table, enter the area code, a non-overlapping range of Office Codes (exchanges), then create a new routing table and specify to keep the last 7 digits and to prepend XXX where XXX is the area code.
- To support 7-digit dialing for the remaining exchanges, add yet another entry in the area code table, enter the area code, leave the Office Code at “Default”, then create another routing table and specify to keep the last 7 digits and prepend nothing.

Configuring specific access profiles

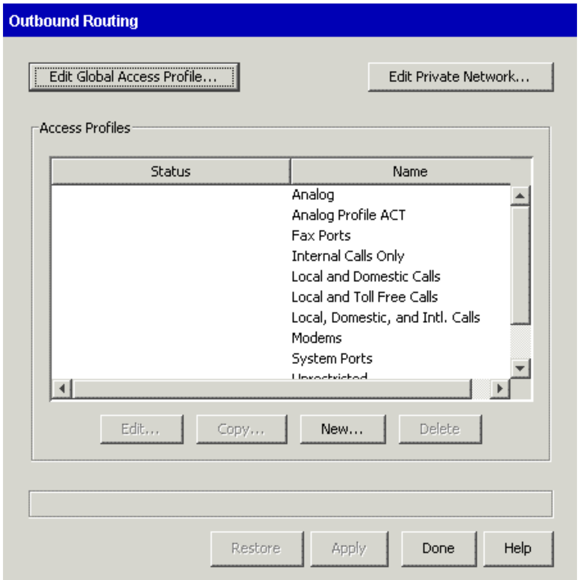
Before going to the Outbound Routing applet, identify the different calling privileges that will be associated with groups of users. From the Outbound Routing applet, you can create, edit, copy, and delete access profiles that you can assign to specific extensions, trunk groups, digital connections, and SIP signaling control points (SCPs). You can edit the existing access profiles or create new ones.

To configure a specific access profile

1 If necessary, click the Administration tab of the Management Console.

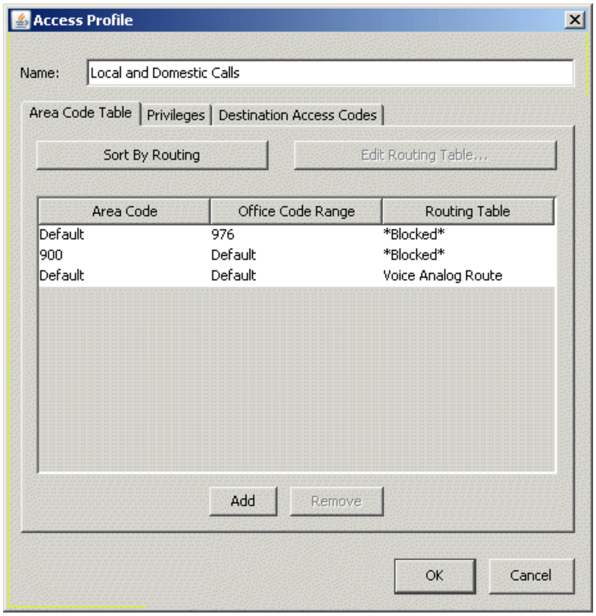
Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.



Status	Name
	Analog
	Analog Profile ACT
	Fax Ports
	Internal Calls Only
	Local and Domestic Calls
	Local and Toll Free Calls
	Local, Domestic, and Intl. Calls
	Modems
	System Ports
	Unrestricted

3 Select an access profile from the list, then click **Edit**, or click **New** to create a new access profile.



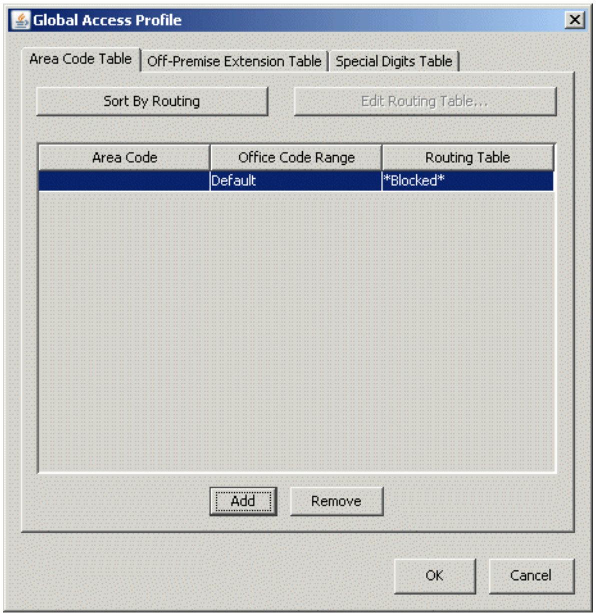
Name: Local and Domestic Calls

Area Code	Office Code Range	Routing Table
Default	976	*Blocked*
900	Default	*Blocked*
Default	Default	Voice Analog Route

In the Area Code Table you can configure Wave to do the following:

- Route calls that do not match rules in the Global Access Profile.
- Specify routing for area code and office code combinations.

4 Click **Add** to add an entry to the Area Code Table. A new record is added to the list.



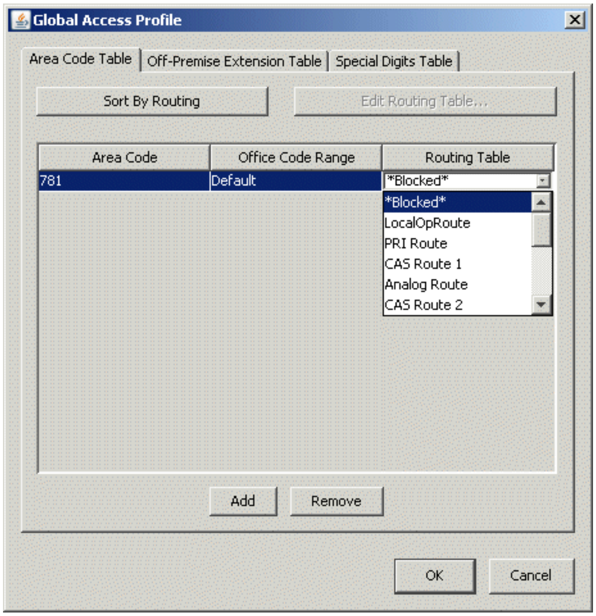
Area Code	Office Code Range	Routing Table
	Default	*Blocked*

5 Edit the **Area Code** and **Office Code Range** for the new area code by double-clicking in each field and entering the codes for which you are providing routing instructions.

- **Area Code**. Enter the area code for which you want to specify routing instructions that apply to all outgoing calls. You might want to add an entry to block outbound calls with an area code of 900. Enter **Default** to allow all area codes.
- **Office Code Range**. Enter the office code (or a range of office codes) within the specified area code. Enter **Default** to match any office code within the specified area code.

6 Click in the **Routing Table** column and select one of the following from the drop-down list:

- A routing table that has already been defined.
- ***Blocked***. Select this option to block all calls to the area or office codes.
- **(New Routing Table)**. Select this option to open the Routing Table dialog. See “Configuring outbound routing tables” on page 9-20 for instructions.

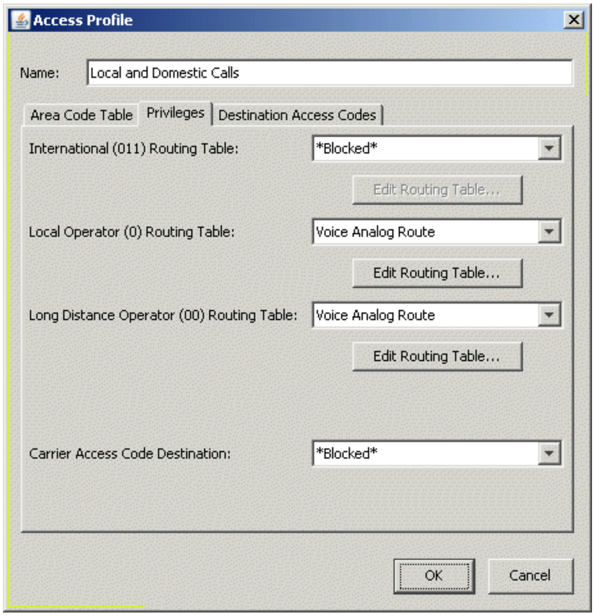


Area Code	Office Code Range	Routing Table
781	Default	*Blocked*

7 Repeat steps 4 through 6 for additional area code and office code routing entries.

8 Click **Sort By Routing** to arrange the rules in the order they should be accessed during call routing.

9 Click the Privileges tab.



Access Profile

Name: Local and Domestic Calls

International (011) Routing Table: *Blocked*

Local Operator (0) Routing Table: Voice Analog Route

Long Distance Operator (00) Routing Table: Voice Analog Route

Carrier Access Code Destination: *Blocked*

The Privileges tab is where you can specify the routing table to which Wave will send calls, depending on the call type. The call type is determined by the first digits entered in the telephone number. You can send calls to different routing tables depending on the following digit strings:

- **011** = International Routing Table
- **0** = Local Operator Routing Table
- **00** = Long Distance Operator Routing Table
- **Carrier Access Code Destination** = A carrier access code is a code (seven digits, beginning with 101) that you dial to access a long-distance carrier, for example 10-10-321.

10 For **International Routing Table**, **Local Operator Routing Table**, and **Long Distance Operator Routing Table**, select one of the following from the drop-down list:

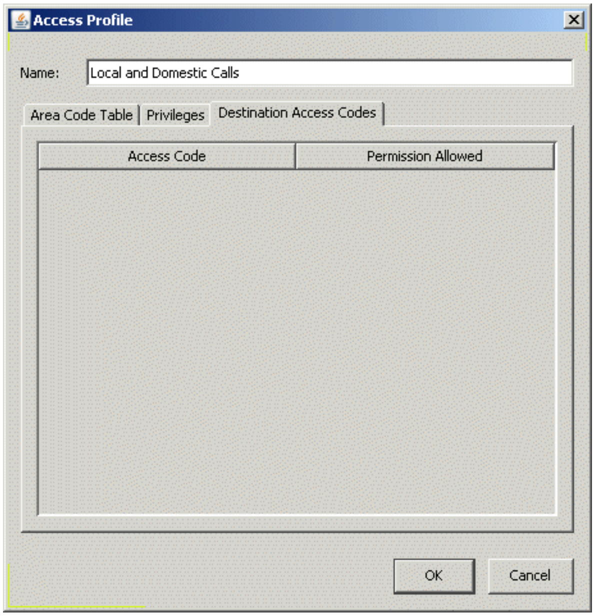
- A routing table that has already been defined.
- ***Blocked***. Select this option to block all calls to the area or office codes.
- **(New Routing Table)**. Select this option to open the Routing Table dialog. See “Configuring outbound routing tables” on page 9-20 for instructions.

To edit the currently-selected routing table, click **Edit Routing Table** to open the Routing Table dialog.

11 For **Carrier Access Code Destination** leave the ***Blocked*** option selected unless you want your users to dial carrier access codes. Otherwise, select one of the following from the drop-down list:

- A trunk group for the call. Note that you cannot assign a routing table to the carrier access code since no translation is required.
- ***Ignored***. This option strips the carrier access code and routes the call as a regular long distance call.

12 Click the Destination Access Codes tab.



Access Profile

Name: Local and Domestic Calls

This tab allows you to specify which external access codes configured in the First Digit Table may be used by this access profile. External access codes may be used to provide access to external paging systems or specific trunks on the Wave Server. (If this tab is blank, you have not configured any external access codes in the First Digit Table.)

13 To allow users with the access profile you are creating or editing to use an access code, select the code in the list and select the **Permission Allowed** check box. To block users with this access profile from using the access code, leave the check box deselected.

14 Click **OK** to close the Access Profile dialog.

15 Click **Apply** to save your changes.

16 Click **Done** to return to the Management Console.

Configuring outbound routing tables

You can access outbound routing tables through the Outbound Routing applet.

To add or edit an outbound routing table

1 If necessary, click the Administration tab of the Management Console.

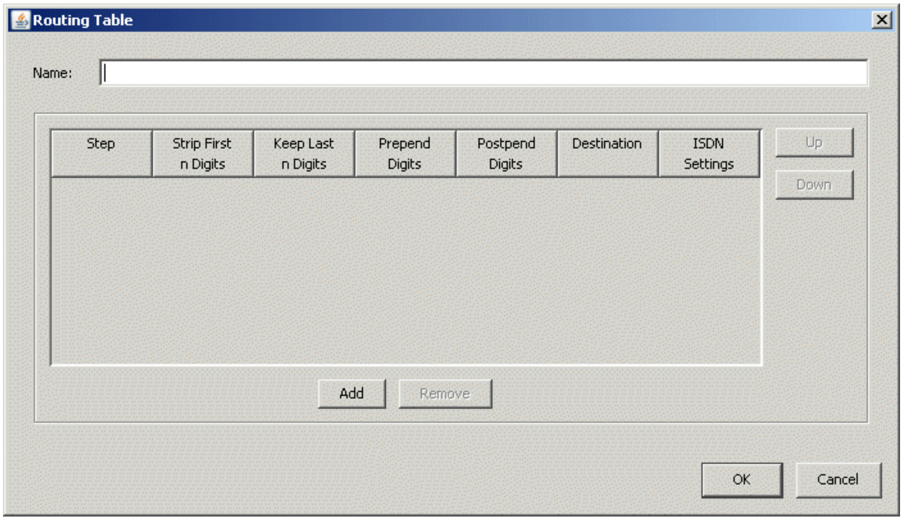
Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

3 Click an **Edit Routing Table** button or choose **(New Routing Table)** from any of the following places.

- Area code tables
- Special digits table
- Off-premise extension table
- Privileges

The Routing Table dialog opens.



4 If this is a new routing table, enter a descriptive **Name**.

5 Click **Add** to add a new step to the routing table.

6 For each step, you can click in the fields and edit the following settings, depending on the translation your CO requires.

- **Strip First n Digits**. Enter the number of digits, if any, that you want to strip from the beginning of the outgoing telephone number.

  Note: The external access code digit (for example, 9) does not need to be stripped. It is not included in any call routing decisions after the call type is determined.

- **Keep Last n Digits**. Enter the number of digits, if any, that you want to keep at the end of the outgoing telephone number.

  Note: For a particular route step, you can enter a value into *either* the **Strip First Digits** *or* **Keep Last Digits** field. Entering 0 for Strip First Digits will not remove any digits. Entering 0 for Keep Last Digits will remove all the digits.

- **Prepend Digits**. Enter the digits that you want to add to the beginning of the outgoing telephone number.
- **Postpend Digits**. Enter the digits that you want to add to the end of the outgoing telephone number.

- **Destination**. Select a destination trunk group (or Signaling Control Point for IP telephony) from the drop-down list. (Signaling Control Points have the following format: `IP`|*Signaling Control Point name*.
- **ISDN Settings**. If you selected a trunk group that is associated with an ISDN trunk in the Trunk Configuration applet, you can select an ISDN setting from the drop-down list. If you do not select a trunk group that is associated with an ISDN trunk, this field is disabled. For more information about how to configure ISDN settings, refer to "Configuring digital channels for ISDN" on page 5-35.

7 Repeat steps 5 and 6 to add steps to the routing table.

8 Click the **Up** or **Down** to move a selected step up or down in the list.

The order of the routing steps is important. Wave tries placing the call to the destination specified in the first step. If the specified trunk is busy, disabled, or disconnected, the system tries the next routing step, and so on. The caller will hear a fast busy tone if all steps have been tried unsuccessfully.

9 Click **OK** to close the Routing Table dialog.

All routing tables are available throughout the Outbound Routing applet. You can use the same routing tables for different outbound routing steps and requirements, but be aware that some places in the applet may require different translation, hence different routing tables.

10 Click **Apply** to save your changes.

11 Click **Done** to return to the Management Console.

Configuring off-premise extension routing

This section provides information about configuring outbound call routing to off-premise extensions. See "Off-premise extensions" on page 29-13 for examples and information about why you might use off-premise extensions. To set up Wave Server to dial off-premise telephone numbers as if they were extensions, you need to complete the following tasks:

- Creating off-premise extension ranges. See page 9-23.
- Configuring the off-premise extension table. See page 9-23.

Creating off-premise extension ranges

Use the procedure “Configuring extension ranges” on page 7-3 to create your off-premise extension ranges if you want to use numbers that begin with a different first digit than those you are using for your local extensions.

For example, if you are using 100-150 for your local extensions and you want to use 159-199 for your off-premise extensions you do not need to configure an additional extension digit in the First Digit Table. Continue with “Configuring the off-premise extension table” on page 9-23.

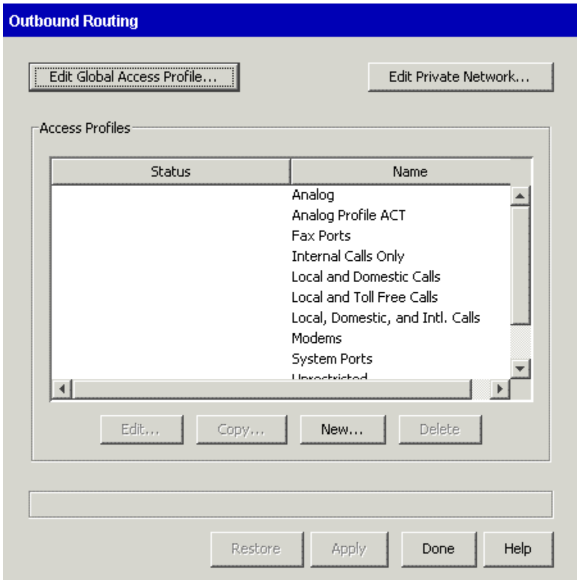
Configuring the off-premise extension table

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

3 The Outbound Routing dialog opens:



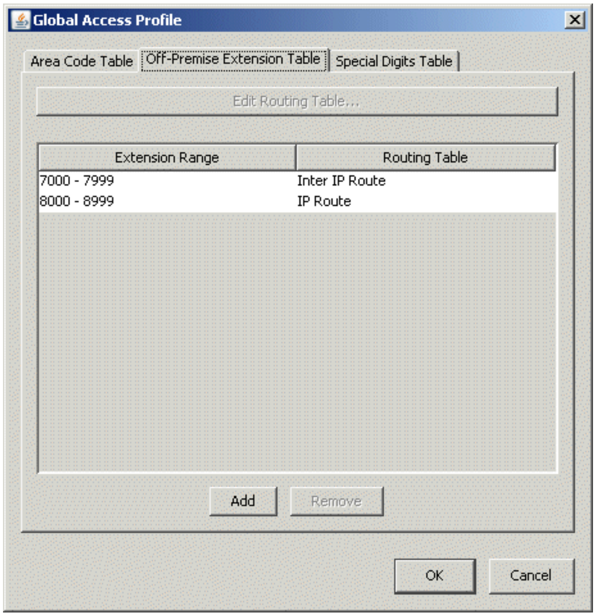
Outbound Routing

Access Profiles

Status	Name
	Analog
	Analog Profile ACT
	Fax Ports
	Internal Calls Only
	Local and Domestic Calls
	Local and Toll Free Calls
	Local, Domestic, and Intl. Calls
	Modems
	System Ports
	Unrestricted

4 Click **Edit Global Access Profile** to open the Global Access Profile dialog.

5 Click the Off-Premise Extension Table tab.



Global Access Profile

Extension Range	Routing Table
7000 - 7999	Inter IP Route
8000 - 8999	IP Route

6 Click **Add** to add a range of off-premise extensions.

A new entry is displayed in the list.

7 Click the **Extension Range** field and enter the range of off-premise extensions you want to configure.

You need to add a new entry for each new range of off-premise extensions.

Note: The First Digit Table must specify the first digit of the off-premise extensions, must have a type of Extension, and must have the same amount of digits as the extensions you specify here.

Note: *Do not* configure off-premise extensions in User/Group Management or the Hunt Groups applet. However, overlap is permitted if you have local extensions that are the same as the off-premise extensions.

8 Create a routing table to translate the digits to go to the telephone company. To do so, click in the **Routing Table** column and select **(New Routing Table)**. See “Configuring outbound routing tables” on page 9-20 for instructions.

9 Click **OK** to close the Global Access Profile dialog, and return to the Management Console.

Configuring destination access code routing

Sometimes you may want to configure a direct access code to a trunk group. Most commonly, this is done to enable users to make outbound calls to access a CO-based paging system.

This section provides information about configuring outbound calls using destination access codes. See “Destination access code/direct to trunk group” on page 29-14 for examples and information about why you might use this type of call routing. To set up Wave to use destination access codes, you need to complete the following tasks:

- Creating destination access codes. See page 9-26.
- Enabling destination access codes. See page 9-27.

Note: By configuring a destination access code to a trunk group instead of via the Outbound Routing applet, there is no way to enforce toll restrictions. Care must be taken to ensure that users who are enabled to use this code (for paging or other functions) will not be able to circumvent other dialing restrictions.

Creating destination access codes

Perform the following steps to create destination access codes in the First Digit Table applet.

To create destination access codes

1 If necessary, click the Administration tab of the Management Console.

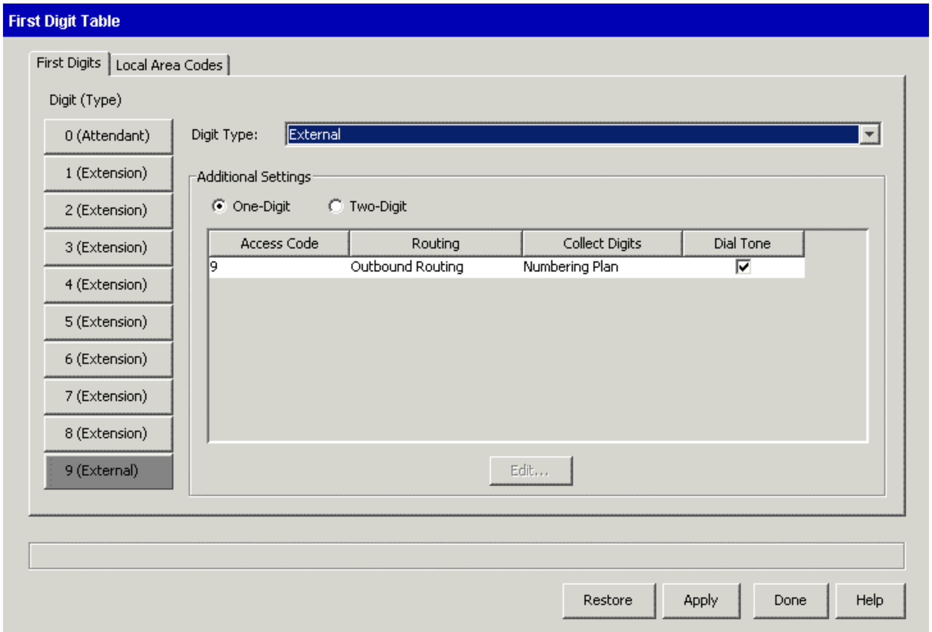
Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 Click the button with the number that you want to configure.

4 Choose **External** from the **Digit Type** drop-down list.

The external digit configuration options appear in the Additional Settings group box.



First Digit Table

Digit Type: External

Additional Settings

● One-Digit ○ Two-Digit

Access Code	Routing	Collect Digits	Dial Tone
9	Outbound Routing	Numbering Plan	☑

5. Specify whether you want this first digit to support **One-Digit** or **Two-Digit** external access codes.

   If you select Two-Digit support, access codes x0 through x9, where *x* is the first digit, appear in the Additional Settings group box.

6. Configure the settings for each access code.
   - **Routing**. Choose the trunk group or IP Signaling Control Point you want to use for routing.
   - **Collect Digits**. Choose one of the following:
     - Specify the number of outgoing digits to collect before the number is sent to the central office. This setting is ideal if you want to limit the number of digits a user can dial using an access code, for example limiting this access code to 11 digits will allow local and long distance calls, but not international calls.
     - Select **Numbering Plan** to collect the digits expected for the numbering plan specific to your locale. For example, the North American Numbering Plan expects telephone numbers to be 7, 10, or 11 digits (when preceded by a 1).
   - **Dial Tone**. Check the Dial Tone check box if you want Wave to provide dial tone after the destination access code is dialed.
   - **VM Networking**. Do not check.

7. Click **Apply** to save your changes.

8. Click **Done** to return to the Management Console.

9. Continue with the instructions in the next section, Enabling destination access codes.

Enabling destination access codes

By default all users are restricted from using new destination access codes. You must enable them in the specific access profiles in the Outbound Routing applet. Enable the access codes only in the specific access profiles that you will assign to groups of users who are permitted to use the codes.

If you haven’t already done so, follow the instructions in the previous section, Creating destination access codes.

To enable destination access codes

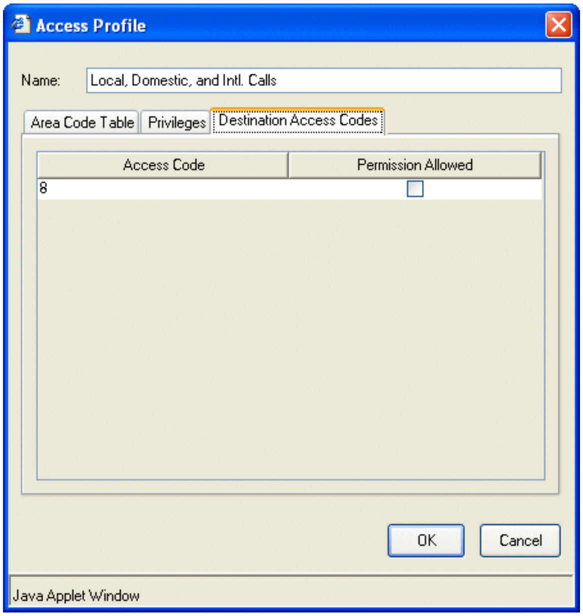
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

3 Select an access profile from the list, then click **Edit**, or click **New** to create a new access profile.

4 Click the Destination Access Codes tab.



Name: Local, Domestic, and Intl. Calls

Access Code	Permission Allowed
8	□

5 Select the **Permission Allowed** check box to enable this access profile to use the specified destination access code.

6 Click **OK** to close the Access Profile dialog.

7 Repeat steps 3 through 6 for each access profile that you want to edit or add.

8 Click **Apply** to save your changes.

9 Click **Done** to return to the Management Console.

Later, when you are configuring extensions and telephones, you will assign specific access profiles to each extension.

Configuring private networking

Configuring private networking is a four-step process. You need to determine a numbering scheme for your private network. You need to configure outbound routing and the First Digit Table to recognize the digits that access the remote Wave systems. Then, you need to go back to the Outbound Routing applet to enable the private networking destination access codes.

The following sections describe how to configure Wave for private networking:

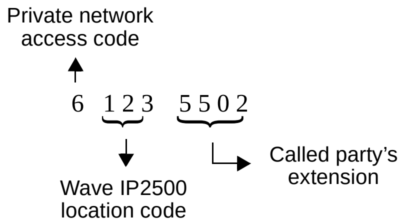
- Determining a numbering scheme for private networking. See page 9-29.
- Configuring outbound routing for private networking. See page 9-30.
- Configuring the First Digit Table for private networking. See page 9-33.
- Enabling the new destination access code. See page 9-37.

Determining a numbering scheme for private networking

Before you can configure your Wave Servers for private networking, you must determine a private networking numbering scheme for your Wave network. The numbering scheme includes the following components:

- **External access code (one or two digits)**. The first one or two digits that you dial to access the private network.
- **Location code (between 2 and 6 digits, inclusive)**. The code that identifies each Wave Server on the network.
- **Extension (between 2 and 7 digits, inclusive)**. The telephone extension for each user.

  The following diagram shows an example of a numbering scheme for private networking:



You need to make decisions about or determine the following things:

- Which external first digit do you want to use for your access code?
- Do you want to use a one-digit or two-digit external access code?
- What length do you want your location codes?

  When you dial within the private network, you will be prepending the location code to the extension of the person you are calling. Be sure to specify a length long enough to accommodate all the Wave Servers on your network. You can specify a location code length of 2, 3, 4, 5, or 6 digits. The default value is 3. A location code cannot start with a 0.

- Determine a Home Location Code for each Wave Server in your network.

Configuring outbound routing for private networking

You need to specify the following information about your private network in the Outbound Routing applet:

- Length of your location codes
- Length of your user extensions
- Home Location Code for this Wave Server.

You also need to specify ranges of location codes and identify the routing table that you want to use with each range.

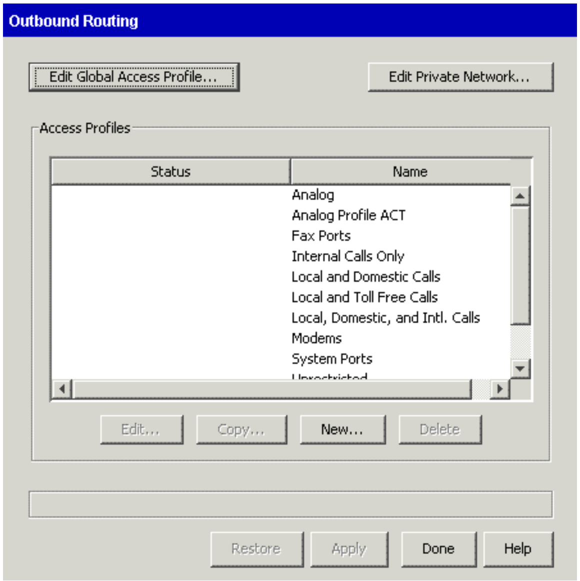
To configure location codes in the Outbound Routing applet

Click

1 If necessary, click the Administration tab of the Management Console.

2 Click the Outbound Routing icon, located in the Trunk Administration section.

3 The Outbound Routing dialog opens.:

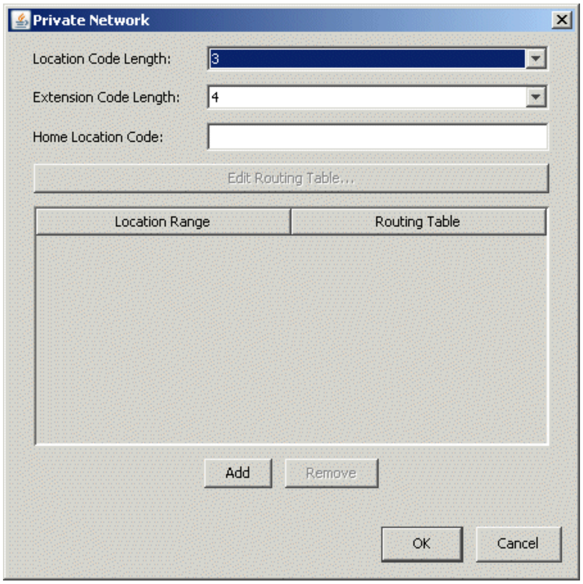


Outbound Routing

Access Profiles

Status	Name
	Analog
	Analog Profile ACT
	Fax Ports
	Internal Calls Only
	Local and Domestic Calls
	Local and Toll Free Calls
	Local, Domestic, and Intl. Calls
	Modems
	System Ports
	Unrestricted

4 Click **Edit Private Network**. The Private Network dialog opens.



Private Network

Location Code Length: 3

Extension Code Length: 4

Home Location Code:

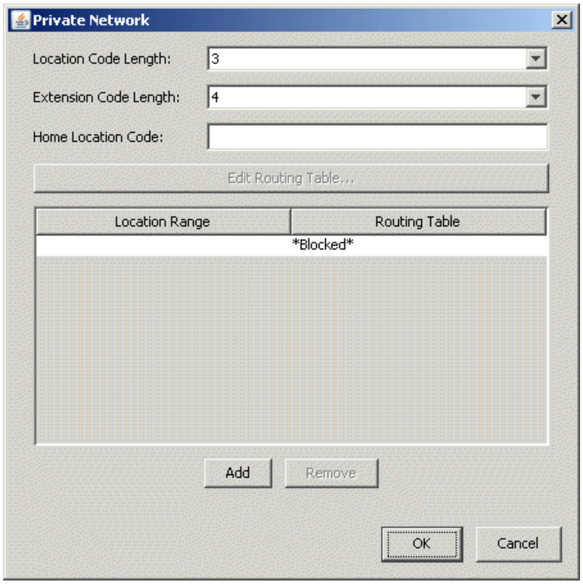
Location Range	Routing Table

5 Select the length you want your location codes to be from the **Location Code Length** drop-down list. Location code length can be 2-6 digits. The default length is 3.

6 Select the length of your Wave extensions in the **Extension Code length** drop-down list.

7 Enter a **Home Location Code** that identifies this Wave Server for internal routing. **Home Location Code** must be the same number of digits as the number you specified for **Location Code Length**.

8 Click **Add** to specify a routing table for a range of location codes. A row is added to the table with a blank **Location Range** and **Routing Table** set to ***Blocked***.



Location Code Length: 3

Extension Code Length: 4

Home Location Code:

Location Range	Routing Table
	Blocked

9 Double-click in the **Location Range** column and enter a range of location codes for which you want to specify a routing table.

Note: You can add multiple ranges of location codes and direct each range to a different routing table.

10 Click in the **Routing Table** column and select one of the following from the drop-down list:

- A routing table that has already been defined.
- ***Blocked***. Select this option to block all calls to the area or office codes.
- **(New Routing Table)**. Select this option to open the Routing Table dialog. See "Configuring outbound routing tables" on page 9-20 for instructions.

11 Click **OK** to return to the Outbound Routing table.

12 Click **Done** to save your changes and return to the Management Console.

Configuring the First Digit Table for private networking

You need to specify which first digit to use to access private networking.

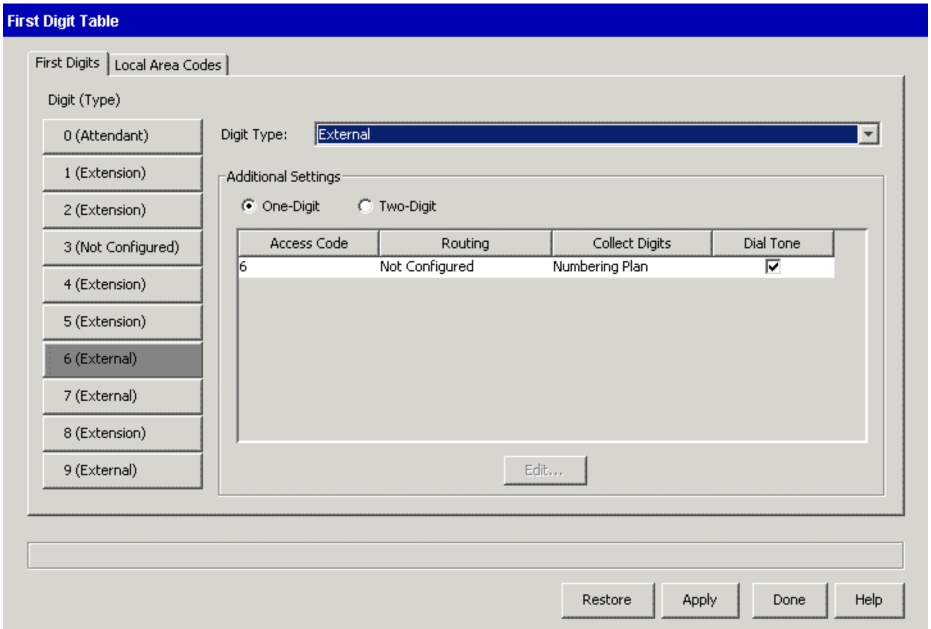
To configure the First Digit Table for private networking

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 In the First Digit Table dialog, select a first digit in the **Digit (Type)** list. If the digit is not already an external digit, select **External** from the **Digit Type** drop-down list.


First Digit Table

First Digits | Local Area Codes

Digit (Type)

- 0 (Attendant)
- 1 (Extension)
- 2 (Extension)
- 3 (Not Configured)
- 4 (Extension)
- 5 (Extension)
- 6 (External)
- 7 (External)
- 8 (Extension)
- 9 (External)

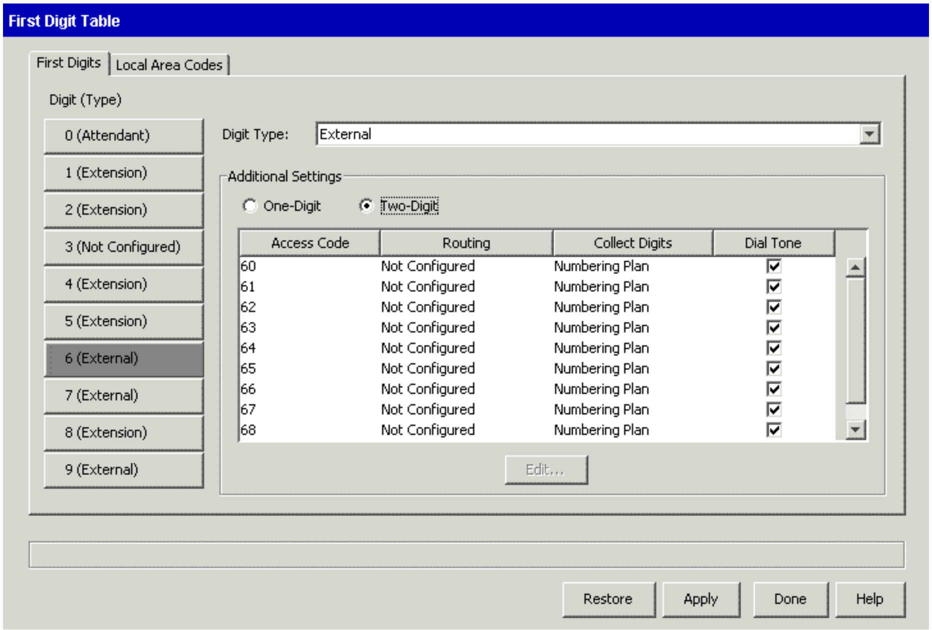
Digit Type: External

Additional Settings

● One-Digit ○ Two-Digit

Access Code	Routing	Collect Digits	Dial Tone
6	Not Configured	Numbering Plan	☑

4 Depending on the type of destination access code you want, select **One-Digit** or **Two-Digit**. If you select **Two-Digit**, access codes *n*0 through *n*9, where *n* is the first digit, appear in the list.



First Digit Table

First Digits | Local Area Codes

Digit (Type)

- 0 (Attendant)
- 1 (Extension)
- 2 (Extension)
- 3 (Not Configured)
- 4 (Extension)
- 5 (Extension)
- 6 (External)
- 7 (External)
- 8 (Extension)
- 9 (External)

Digit Type: External

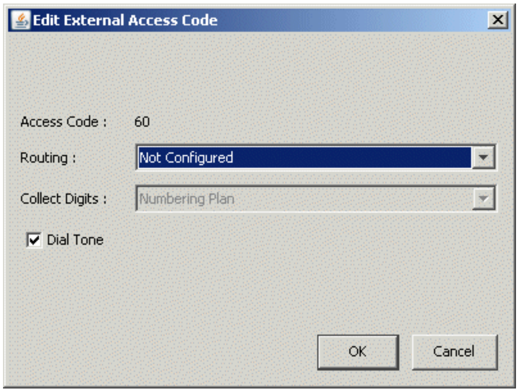
Additional Settings

○ One-Digit ● Two-Digit

Access Code	Routing	Collect Digits	Dial Tone
60	Not Configured	Numbering Plan	☑
61	Not Configured	Numbering Plan	☑
62	Not Configured	Numbering Plan	☑
63	Not Configured	Numbering Plan	☑
64	Not Configured	Numbering Plan	☑
65	Not Configured	Numbering Plan	☑
66	Not Configured	Numbering Plan	☑
67	Not Configured	Numbering Plan	☑
68	Not Configured	Numbering Plan	☑

5 Select the **Access Code** that you want to configure, then click **Edit**.

The Edit External Access Code dialog opens.



Edit External Access Code

Access Code : 60

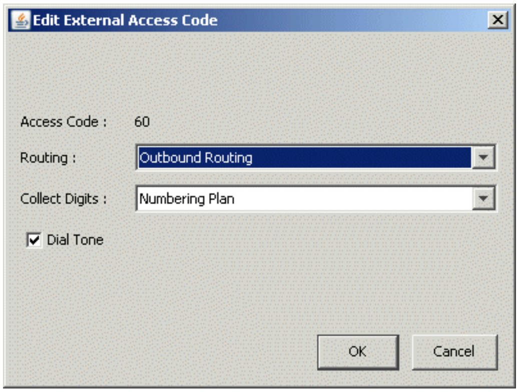
Routing : Not Configured

Collect Digits : Numbering Plan

☑ Dial Tone

Note: The **Collect Digits** field remains grayed out until you select a routing table from the **Routing** drop-down list.

6 Select **Outbound Routing** from the **Routing** drop-down list.



Edit External Access Code

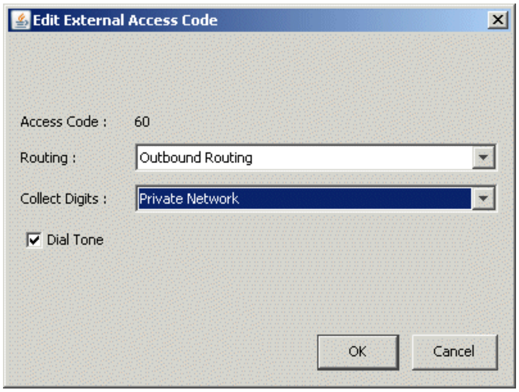
Access Code : 60

Routing : Outbound Routing

Collect Digits : Numbering Plan

☑ Dial Tone

7 Select **Private Network** from the **Collect Digits** drop-down list.



Edit External Access Code

Access Code : 60

Routing : Outbound Routing

Collect Digits : Private Network

☑ Dial Tone

8 Click **OK** to return to the First Digit Table applet.

9 If you are configuring multiple external access codes, repeat steps 5 through 8 for each.

10 Click **Done** in the First Digit Table applet to save your changes and return to the Management Console.

Enabling the new destination access code

Every external first digit that is configured in the First Digit Table for a private network is displayed in the Destination Access Codes tab of the Access Codes dialog in the Outbound Routing applet. By default, an access profile does not allow access to a destination access code until permission is granted by the system administrator.

If there are users that do not need access to your private network, you can set up an Access Profile for those users and not grant permission for the new destination access code(s).

So, the last step in configuring private networking is to grant permission for the new destination access code.

To enable the new destination access codes

1 If necessary, click the Administration tab of the Management Console.

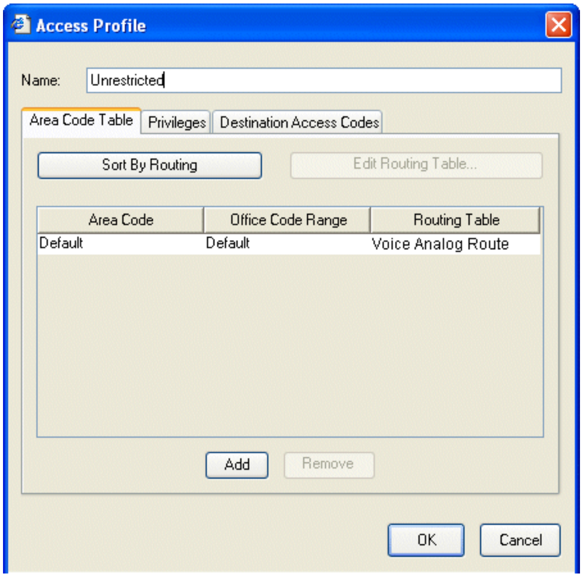
Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

The Outbound Routing applet starts.

3 Select the access profile you want to configure for private networking, then click **Edit**.

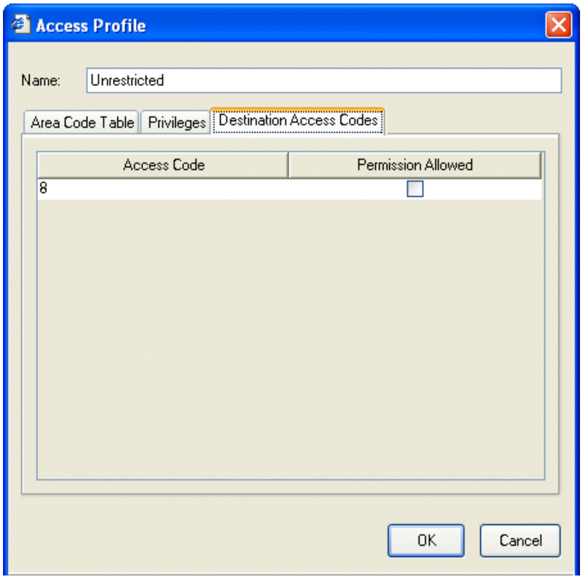
Alternatively, you can select **New** to add an access profile. Refer to “Configuring specific access profiles” on page 9-14 for information about adding access profiles.



Name: Unrestricted

Area Code	Office Code Range	Routing Table
Default	Default	Voice Analog Route

4 Select the Destination Access Codes tab.



Name: Unrestricted

Access Code	Permission Allowed
8	□

5 Select the **Permission Allowed** check box for each access code for which you want to grant permission for the selected access profile.

6 Click **OK** to return to the Outbound Routing applet.

7 Click **Done** in the Outbound Routing applet to save your changes and return to the Management Console.

Changing an access code in a user's saved numbers

When a user saves phone numbers in ViewPoint that can be speed-dialed or auto-dialed, the dialing service used to make the call is saved with them. Such numbers include contact phone numbers and the phone numbers specified in call forwarding and routing lists. You can do a global replace of one dialing service for another across all users' saved numbers. For example, you can specify that all numbers saved with the "9 - Phone number" service now use your "8 - Centrex" service.

To replace all occurrences of one saved dialing service with another

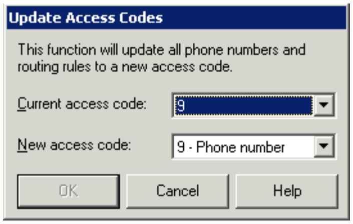
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section. The User/Group Management applet opens.

See "Using the User/Group Management applet" on page 2-15 for information about navigating in the User/Group Management applet.

3 Choose **Tools > Update Access Codes.** The Update Access Codes dialing box opens.



Update Access Codes

This function will update all phone numbers and routing rules to a new access code.

Current access code: 9

New access code: 9 - Phone number

4 Choose the dialing service you want to replace under **Current access code** and the dialing service you want to replace it with under **New access code**.

5 Click **OK.** All phone numbers that users have entered in theWave database with the **Current access code** are changed to use the **New access code**.

Setting default access codes for callbacks

When users return calls or voice messages using the telephone commands or ViewPoint, the system automatically uses a default access code.

To set a default access code for callbacks

1 If necessary, click the Administration tab of the Management Console.

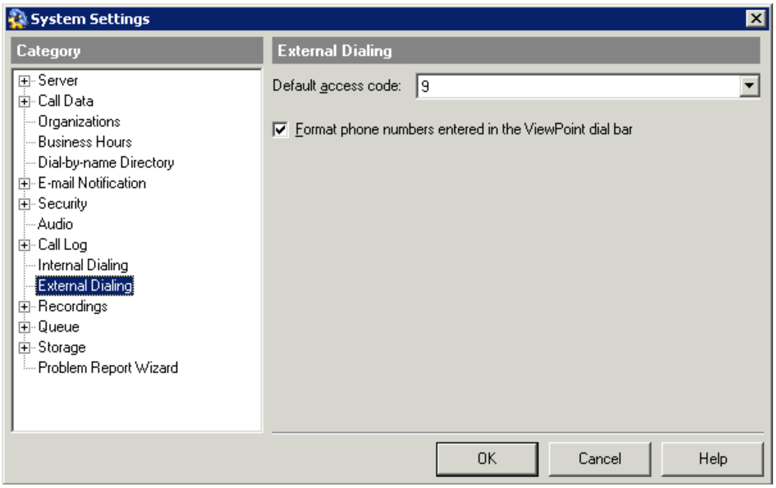
Click

2 Click the User/Group Management icon, located in the PBX Administration section. The User/Group Management applet opens.

See “Using the User/Group Management applet” on page 2-15 for information about navigating in the User/Group Management applet.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the External Dialing tab.



Default access code: 9

☑ Format phone numbers entered in the ViewPoint dial bar

5 From the **Default access code** drop-down list, select the access code for the dialing service that will be used to return a call from a phone number from the Call Log and Voice Messages views. The default is 9. You can select a routing service or any dialing service that takes phone numbers as inputs. You typically would use a routing service or a Phone Number dialing service.

6 Click **OK**.

Where the default access codes are displayed

In the User/Group Management applet, the Default column of the Dialing Services view shows the current defaults for phone number and Internet callbacks.

In ViewPoint, the Place Call To dialog always opens with the current default dialing service for phone numbers selected (the user can also choose a different dialing service to place a call). When you import contacts, new phone numbers and IP addresses automatically receive the default access codes.

Dialing phone numbers entered in the ViewPoint dial bar exactly as entered

This procedure is primarily of interest for systems located in EU countries. To support EU dialing requirements, Wave allows phone numbers entered via the ViewPoint dial bar to be dialed as entered including access code, without any formatting, exactly as if the user entered the same digits from the phone.

Note: In the current version, this checkbox is *incorrectly* selected by default whenever a non-North American locale is specified.

Typically, for North American systems formatting rules are applied to numbers entered in the ViewPoint dial bar—this is the default setting, and does not need to be changed as described in the following steps.

To dial phone numbers exactly as entered in the ViewPoint dial bar

1 If necessary, click the Administration tab of the Management Console.

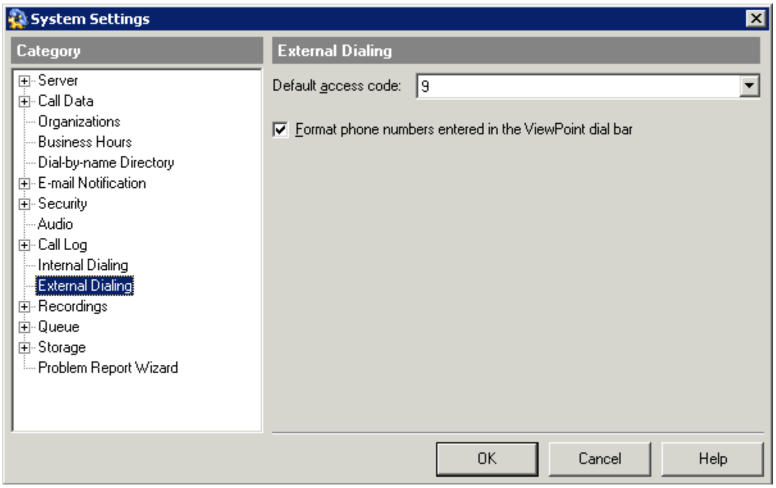
Click

2 Click the User/Group Management icon, located in the PBX Administration section. The User/Group Management applet opens.

See “Using the User/Group Management applet” on page 2-15 for information about navigating in the User/Group Management applet.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the External Dialing tab.



Default access code: 9

☑ Format phone numbers entered in the ViewPoint dial bar

5 Deselect the **Format phone numbers entered in the ViewPoint dial bar** checkbox. (If this checkbox is selected, which is by default, numbers entered via the ViewPoint dial bar will be reformatted according to the dialing rules you have set up.)

Setting up emergency dialing

Wave supports various emergency dialing scenarios:

- In North America, standard 911 emergency dialing service does not require additional hardware. All standard 911 calls use a Wave trunk and go through the phone company to the emergency dispatching center. A user can make an emergency call from any Wave phone (including from a phone that is not assigned to any user), even if the user is blocked from making external calls.
- On EU systems, users typically dial 112 to access emergency services. No dialing prefix is required to make emergency calls, and Caller ID is never blocked.

You can further customize emergency dialing by defining one or more emergency numbers in the Special Digits Table of the Global Access Profile. There is no limit to the number of entries that can be configured as emergency numbers. See “Defining emergency numbers” on page 9-43

Note: Emergency numbers were handled differently prior to Wave ISM 2.0. If you upgrade from an earlier version, any emergency numbers that you configured previously will be displayed in the Special Digits Table and flagged as emergency numbers.

Requiring users to dial an access code before dialing an emergency number

In order to help prevent accidental emergency calls, Wave is configured by default to require users to dial an external access code before dialing an emergency number. You can turn this option off so that users can dial an emergency number directly. For more information, see “Requiring an access code for emergency number dialing” on page 16-13

Defining emergency numbers

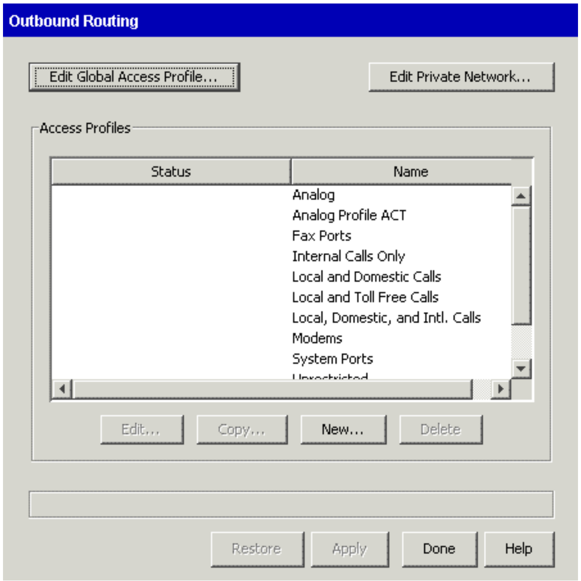
Perform these steps to define one or more emergency numbers:

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the Outbound Routing icon, located in the PBX Administration section. The General Settings applet opens.

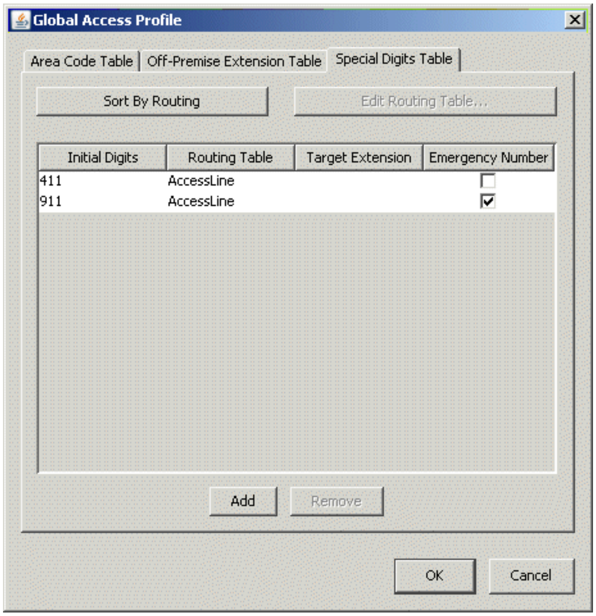
3 The Outbound Routing dialog opens:



Analog
Analog Profile ACT
Fax Ports
Internal Calls Only
Local and Domestic Calls
Local and Toll Free Calls
Local, Domestic, and Intl. Calls
Modems
System Ports
Unrestricted

4 Click **Edit Global Access Profile** to open the Global Access Profile dialog.

5 Click the Special Digits Table tab.



Initial Digits	Routing Table	Target Extension	Emergency Number
411	AccessLine		☐
911	AccessLine		☑

You use the Special Digits Table to enter any digits or strings of digits that you want Wave to process before processing the rules in the other tables. For complete details on how to use this table, including adding new entries, see "Configuring the Global Access Profile" on page 9-4.

6 Select the **Emergency Number** checkbox for any **Initial Digits** entry that you want to be processed as an emergency number. You can select all of the entries in the table.

Note: At least one entry in the Special Digits Table must be flagged as an emergency number. If not, an error message is displayed when you try to close this dialog.

7 Click **OK**. Your changes will take effect the next time that the Wave Server is restarted.

Chapter 10

Configuring Phones

CHAPTER CONTENTS

You can customize phone behavior in several ways:

- **Via the User Configuration (Templates) applet.** Phone behavior defined via a template is applied to all users who are assigned that template. If you have groups of users who use the same phone model and who require a similar set of phone features, you can create a template for those users in the User Configuration (Templates) applet that associates those features with buttons on the phone. This chapter explains how to view, create, and modify phone templates for analog, digital, and SIP phones.

  Hint: Once you create or refine a phone template, you can then assign it to a user when you create the user. For this reason you should define phone templates before creating users.

- **Via the User/Group Management applet.** Phone behavior defined via the User dialog / Station Features tab applies only to that user's phone. Use the User/Group management applet to make specific overrides to an assigned phone template for an individual user's phone. See “The Phone tab” on page 11-58 for details.
- **Via the phone**. Users can customize some aspects of their own phone's behavior from the phone itself. See the *Wave Phone User Guide* for more information.

About phone templates

Depending on the phone type, the corresponding phone template controls different aspects of phone behavior.

- Analog phone templates define the physical capabilities of the phone, such as message waiting indicator or Caller ID display.
- Digital and SIP phone templates define feature button behavior, such as Auto Dial or Outside Line, for those respective phone types.

Configuring phone templates

This section describes how to do the following:

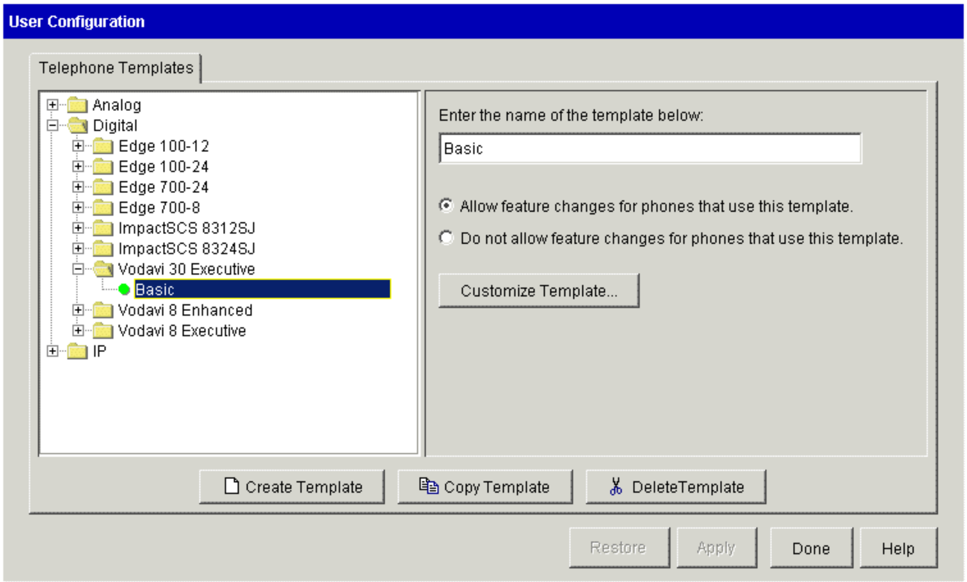
- View phone templates. See page 10-3.
- Create a new template. See page 10-4.
- Copy an existing template. See page 10-4.
- Customize an analog phone template. See page 10-5.
- Customize a digital phone template. See page 10-7.

To view phone templates

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User Configuration (Templates) icon, located in the PBX Administration section. The User Configuration applet opens displaying the Telephone Templates tab.



User Configuration

Telephone Templates

- Analog
- Digital
  - Edge 100-12
  - Edge 100-24
  - Edge 700-24
  - Edge 700-8
  - ImpactSCS 8312SJ
  - ImpactSCS 8324SJ
  - Vodavi 30 Executive
    - Basic
  - Vodavi 8 Enhanced
  - Vodavi 8 Executive
- IP

Enter the name of the template below: Basic

● Allow feature changes for phones that use this template.

○ Do not allow feature changes for phones that use this template.

3 Click one of the folders in the left pane.

- **Analog**. Contains templates for each analog phone configuration supported on Wave (see “Customizing analog phone templates” on page 10-4 for a description of each configuration.)
- **Digital**. Contains a folder with templates that include preprogrammed feature buttons for each of the supported Wave digital phone models.
- **IP**. Contains templates for each of the SIP phone types that have been certified for use with Wave.

To create a new template

1. Select a template folder or template.
2. Click **Create Template**.
3. Select the new template and rename it in the field in the right pane.

To copy an existing template

1. Select one of the templates.
2. Click **Copy Template** to create a copy of the selected template.

   A new template is displayed at the bottom of the template list.
3. Select the new template and rename it in the field in the right pane.

Customizing analog phone templates

If you use analog phones on your Wave system, there are seven default templates provided that contain most combinations of analog phone Caller ID and message waiting indicator feature options. There is a Fax modem template provided as well. Typically, you will not need to change the templates, but you do need to select the correct one when you create a new user.

The default analog phone templates are:

- **Basic - Lamp**. Use for phones with no Caller ID and a message waiting lamp.
- **Basic - Stutter**. Use for phones with no Caller ID and no message waiting lamp.
- **Caller ID - Lamp**. Use for phones with Caller ID and a message waiting lamp.
- **Caller ID - Stutter**. Use for phones with Caller ID and no message waiting lamp.
- **Enhanced Call Waiting - Lamp**. Use for phones with enhanced Caller ID and a message waiting lamp.
- **Enhanced Call Waiting - Stutter.** Use for phones with enhanced Caller ID and no message waiting lamp.

- **External Voicemail / External Fax Server**. Use for extensions connected to external voicemail systems and external fax servers.

  Note that using this template has the effect of sending AT&T System 25 DTMF codes to an extension connected to an external voice mail system or external fax server when it picks up the call. The DTMF digits is sent using the following format:

  #<opcode>#<sourceNumber>#<destinationNumber>#

  The opcodes are 00 for direct internal call, 01 for direct external call, 02 for forwarded internal calls, and 03 for forwarded external calls. For example, if you dial one of these extensions from an internal extension x123, it would get the digits “#00#123##”. If it were an external call forwarded from an internal x123, you would see “#03##123#”.

Important! Your fax server may not recognize opcodes and may only require the DID number from the PSTN. If this is the case, do NOT select the **External Voicemail/External Fax Port** template for the port, but instead select the **Basic - Stutter** template. This may also be true if you are using certain media gateways to translate analog fax tone to T.38 fax-over-IP. Those gateways may require alteration of their parsing systems to handle or process even basic DID and/or opcode strings. Vertical recommends that you keep things as simple as possible and not use the **External Voicemail/Fax Server Port** template unless your device specifically requires opcodes.

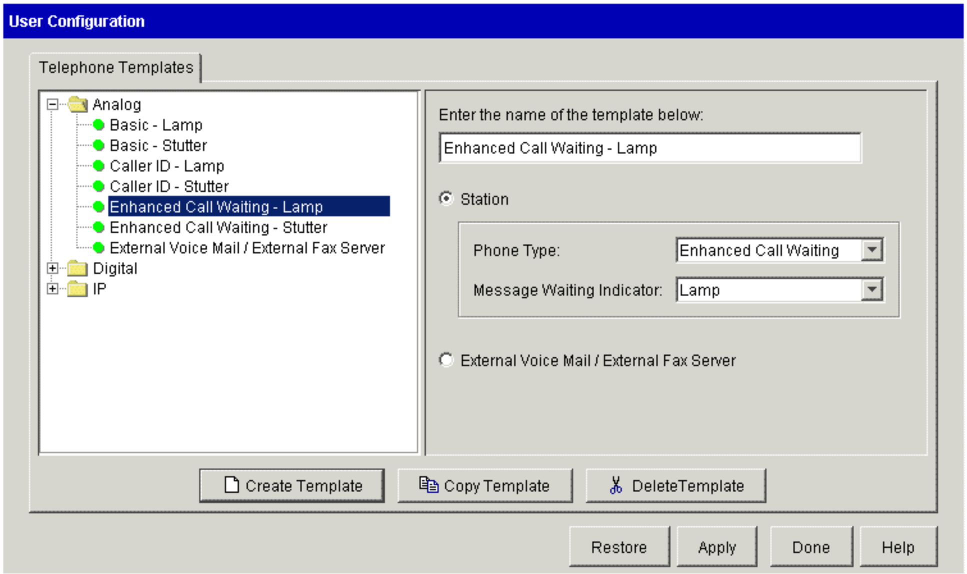
To customize an analog phone template

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User Configuration (Templates) icon, located in the PBX Administration section.

3 Select one of the analog phone templates.



User Configuration

Telephone Templates

- Analog
  - Basic - Lamp
  - Basic - Stutter
  - Caller ID - Lamp
  - Caller ID - Stutter
  - Enhanced Call Waiting - Lamp
  - Enhanced Call Waiting - Stutter
  - External Voice Mail / External Fax Server
- Digital
- IP

Enter the name of the template below: Enhanced Call Waiting - Lamp

● Station

Phone Type: Enhanced Call Waiting

Message Waiting Indicator: Lamp

○ External Voice Mail / External Fax Server

4 Select the device for which this template will be used:

- **Station**. Analog phone used for making and receiving voice communications.
- **External Voicemail/External Fax Server**. Analog connection for an external voicemail system or external fax server. If you select this option, go to step 7.

5 Select a **Phone Type** from the drop-down list.

- **Basic**. Select this option if this phone cannot display Caller ID, or if Caller ID is not supplied by your phone service provider.
- **Caller ID**. Select this option if this phone type can display Caller ID on inbound calls when the phone is idle.
- **Enhanced CW**. Select this option if this phone type can display Caller ID on inbound calls when the phone is idle and also on call waiting calls.

6 Select a **Message Waiting Indicator** from the drop-down list.

- **Lamp**. Select this option if this phone has a lamp that lights when new messages arrive in the user’s voice mailbox.
- **Stutter**. Select this option if this phone provides a stutter dial tone when new messages arrive in the user’s voice mailbox.

7 Click **Done** to save your changes, and return to the Management Console.

Customizing digital and SIP phone templates

Wave includes one or more default phone templates for each supported digital and SIP phone model. You can customize these defaults as follows:

- Each supported digital phone model has one or more templates that include pre-configured feature buttons (for example, Basic, Operator, Multiple Call Appearance, and so forth) that you can customize further for different types of digital phone users, or you can create new templates.
- Each supported SIP phone model has a default template that you can use to create new, customized templates.

To customize a digital phone or SIP phone template

1 If necessary, click the Administration tab of the Management Console.

Click

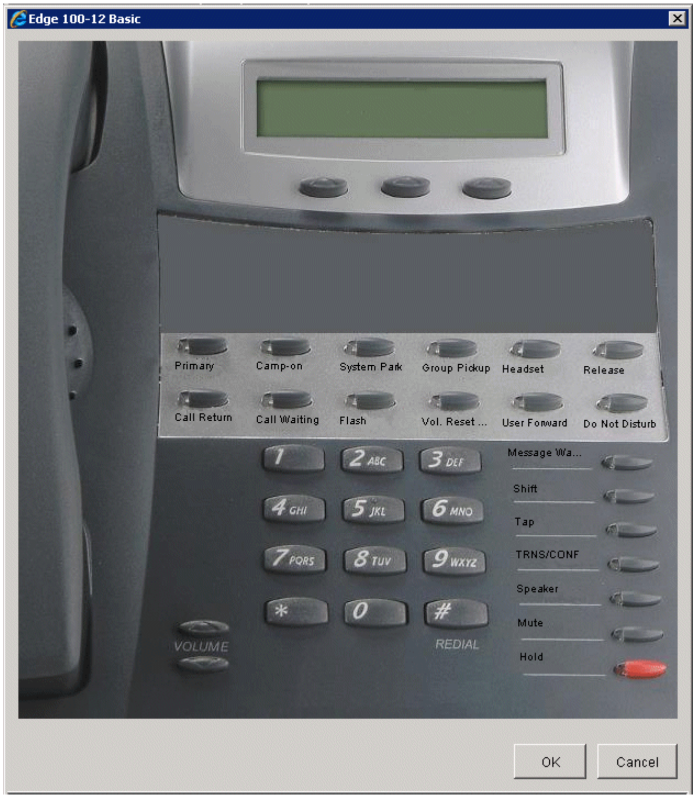
2 Click the User Configuration (Templates) icon, located in the PBX Administration section.

3 Expand **Digital** or **IP** in the left pane, and then select one of the digital or SIP phone templates. (To select a digital phone template, first expand the phone model to view the available templates.)

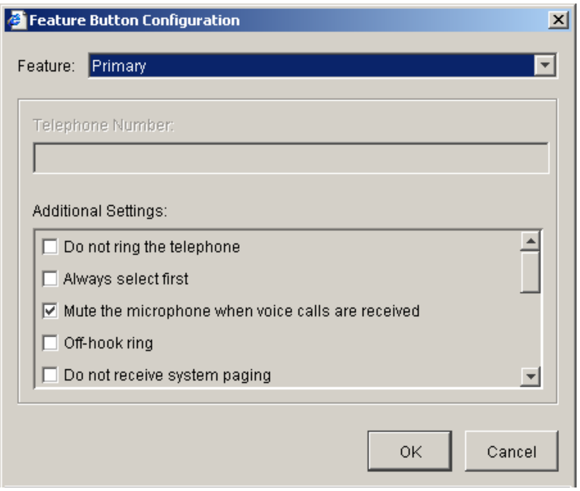
4 Specify whether to allow feature changes for phones that use this template.

- **Allow feature changes for phones that use this template**. Select this option to allow users to reassign feature buttons via the phone, or if you want to be able to change feature button assignments for individual users via the User dialog / Station Features tab in the User/Group Management applet. (Changes made via the Station Features tab only affect the feature button assignment for the individual user, and do not affect the template itself.)
- **Do not allow feature changes for phones that use this template**. Select this option if you want feature button assignments to be controlled by the template, with no other changes allowed.

5 Click **Customize Template** in the right pane. A graphical representation of the phone is displayed with descriptions of the pre-programmed feature buttons displayed on the phone. The following example shows the Telephone Template dialog for the Edge 100-12 digital phone.



6 Click the text on a feature button in the graphic to change the feature assigned to that button. The Feature Button Configuration dialog opens.



Feature Button Configuration

Feature: Primary

Telephone Number:

Additional Settings:

☐ Do not ring the telephone

☐ Always select first

☑ Mute the microphone when voice calls are received

☐ Off-hook ring

☐ Do not receive system paging

7 Select the feature to assign from the **Feature** drop-down list. Some features have additional settings such as **Do not ring the telephone**, **Do not allow break-in**, and so forth.

Hint: Right-click a button description on the phone template to open a shortcut menu with the features available for the button. If you select a feature that requires additional information, the Feature Button Configuration dialog opens.

See “Configuring digital and SIP phone feature buttons” on page 10-10 for information about default, required, and optional settings for each of the programmable features.

8 Click **OK** to finish configuring the feature button and close the Feature Button Configuration dialog.

9 Click **OK** to close the graphical representation of the phone.

10 Click **Apply** to save your changes.

11 Click **Done** to return to the Management Console.

Configuring digital and SIP phone feature buttons

This section lists the features that you can assign to feature buttons on Vertical digital and SIP phones. The following information is provided for each feature.

- **Description**
- **Phone type**. Whether the feature is supported on analog, digital, or SIP phones.
- **Required settings**
- **Optional settings**
- **Important notes**. Additional information about the feature, including how a feature may interact with other features.

Available digital and SIP phone features

The following table lists the features that you can assign to phone feature buttons. Note that not all features are available on SIP phones, or on all digital phone models. If a feature is not available for a specific phone, it is not displayed in the **Feature** drop-down list in the Feature Button Configuration dialog when you edit that phone's template.

Feature	Digital phone	SIP phone	See page
Agent Login	Yes	No	10-12
Agent Status	Yes	No	10-13
Auto Dial	Yes	Yes	10-13
Call Appearance	Yes	Yes	10-14
Call Record	Yes	No	10-15
Call Return	Yes	No	10-16
Call Waiting	Yes	No	10-16
Camp-on (Callback)	Yes	No	10-17
Centrex Flash	Yes	No	10-17
Conference	Yes	No	10-17

Feature	Digital phone	SIP phone	See page
DSS/BLF	Yes	No	10-18
Directed Park	Yes	Yes	10-19
Do Not Disturb	Yes	No	10-20
Extension Pickup	Yes	No	10-20
Flash	Yes	No	10-20
Group Pickup	Yes	Yes	10-21
Headset	Yes	No	10-21
Hold	Yes	No	10-22
Line Appearance	Yes	Yes	10-22
Message Waiting	Yes	Yes	10-25
Mute	Yes	No	10-25
Night Answer	Yes	No	10-26
Outside Line	Yes	No	10-26
Page	Yes	Yes	10-27
Primary	Yes	Yes	10-27
Privacy	Yes	No	10-30
Program	Yes	No	10-30
Queue Status	Yes	No	10-31
Redial	Yes	No	10-32
Release	Yes	No	10-32
Restrict	Yes	No	10-33
Save/Repeat	Yes	No	10-33
Self Park	Yes	Yes	10-33
Shift	Yes	No	10-34

Feature	Digital phone	SIP phone	See page
Silent Monitor	Yes	No	10-34
Speaker	Yes	No	10-35
System Speed Dial	Yes	Yes	10-35
System Park	Yes	Yes	10-36
Tap	Yes	No	10-37
Transfer	Yes	No	10-37
TRNS/CONF	Yes	No	10-38
Unassigned	Yes	Yes	10-38
User Forward	Yes	No	10-39
Voice Call	Yes	Yes	10-40
Volume Reset Override	Yes	No	10-41
Wave Phonebook	No	Yes	

Agent Login feature

Dials the Call Navigator or queue, and then logs the phone in as an agent. When the LED is green, the agent is logged in. When the LED is off, the agent is logged out.

Note: Pressing a configured Agent Login button on a digital phone will have no effect unless the Wave Call Navigator is installed.

Phone type: Digital.

Required settings:

- **Extension**. Extension number of the Call Navigator application or queue.

Optional settings: None.

Agent Status feature

Lets an agent toggle his or her state between Forced-not-ready and Ready, or between Not Ready and Ready. The phone's LED displays the agent's state as follows:

- Green = Ready (idle).
- Red = Not Ready or Forced Not ready.
- Flashing Red = Forced not ready (will take effect when current call completes).

Note: Pressing a configured Agent Status button on a digital phone will have no effect unless the Wave Call Navigator is installed.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Auto Dial feature

Automatically dials a specified phone number. You can include multiple Auto Dial buttons on a phone, including shifted Auto Dial buttons (see "Shift feature" on page 10-34.)

Phone type: Digital, SIP.

Required settings: None.

Optional settings:

- **Telephone Number**. Include any digit sequence up to 32 digits. If you leave this field blank, the user can program an auto dial number from the phone. See the *Wave Phone User Guide* for instructions.
- **Allow application control of LED**. If checked, a custom TAPI application (such as Call Navigator) will control the phone's LED, for example to alert the user to service a call.

Note the following:

- If you select this option for an Auto Dial feature button, a user will not be able to reassign the button using the phone.
- This setting cannot be applied to a shifted Auto Dial button.

- **Add Flash**. If checked, the phone will simulate the FLASH button being pressed prior to dialing the phone number.

Call Appearance feature

Acts as another instance of the phone's Primary button, allowing the user to handle multiple calls to the same extension. For example, if a user's phone has the Primary button assigned to extension 201, and two Call Appearance buttons, then 3 calls to extension 201 will be delivered to the phone, and the user can see the status of each one (ringing, connected, on hold) by looking at those 3 buttons. With multiple active calls, pressing the Call Appearance button switches between the calls, thereby placing the other calls on hold.

You can include multiple Call Appearance buttons on a phone.

Phone type: Digital, SIP.

Required settings: None.

Optional settings: None.

Important notes:

- **Call Appearance and Call Waiting:** If there is one or more Call Appearance buttons configured on a phone, a Call Waiting button should not be configured. It is preferable to use Call Appearance buttons to answer additional calls to the extension rather than a Call Waiting button because a Call Appearance button shows the call status on the phone's display, while a Call Waiting button does not. Also, once connected you can move easily between calls by pressing the associated Call Appearance buttons.

  Note that call waiting is automatically enabled for a user if that user's phone configuration includes a Call Waiting feature button.

- **Call Appearance and Line Appearance:** You cannot configure a Call Appearance button on a phone if that phone's primary extension is already mapped to a Line Appearance button on another phone. Similarly, you cannot configure a Line Appearance button mapped to an extension that is already configured as a Call Appearance button on that extension's primary phone.

  If either of these configurations are detected when you are editing a user or applying a digital or SIP phone template, Wave displays an error message and does not allow the button to be configured or the template to be applied.

Note: Previous versions of Wave allowed these feature button configurations, and users with the unsupported configurations may still exist in your Wave database. If you are editing one of these users, the unsupported configuration will now prevent the user from being saved even if you made no changes to feature button assignments. If this problem occurs, either remove the Line Appearance button, or remove the Call Appearance button from the primary phone of the extension to which you want to map the Line Appearance button.

Call Record feature

Records the current call and saves the recording as a voicemail message. You can include one Call Record button per phone.

Phone type: Digital.

Required settings: None.

Optional settings:

- **Mailbox**. Extension where call recordings will be saved as voicemail messages.

Warning! *In some localities, it is illegal to record a phone call without first notifying the person who is being recorded.*

Call Return feature

Calls back the extension from which the last inbound call on the primary line appearance came, if the call originated on the local Wave system. You can include one Call Return button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Call Waiting feature

Places the active call on hold and connects to an incoming call. You can include one Call Waiting button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Important notes:

- It is preferable to configure one or more Call Appearance buttons to answer additional calls rather than a Call Waiting button, because a Call Appearance button shows the call status on the phone’s display, while a Call Waiting button does not. Also, once connected you can move easily between calls by pressing the associated Call Appearance buttons.
- Call waiting is automatically enabled for a user if that user’s phone configuration includes a Call Waiting feature button.

Camp-on (Callback) feature

Automatically calls back an extension that is busy, does not answer, or is forwarding calls to voicemail when the extension becomes available. You can include multiple Camp-on buttons on a phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Centrex Flash feature

Accesses a Centrex feature, if you use Centrex. Centrex is a PBX-like service that provides switching at the phone company’s central office instead of at your own premises.

Pressing the Centrex Flash feature button signals the Centrex system that you intend to use a special feature. For example, pressing the Centrex Flash feature button while on a call followed by another Centrex number transfers the call to that number. For details on how to use Centrex, see the documentation made available by your Centrex provider.

You can include one Centrex Flash button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Conference feature

Creates and adds internal and external parties to a conference call. You can include one Conference button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Direct Station Select/Busy Lamp Field (DSS/BLF) feature

Monitors the state of a specific extension, and provides a quick way to call or transfer a call to that extension.

- A solid red LED next to a DSS/BLF button indicates that the monitored extension is in use.
- A flickering red LED indicates the monitored extension is ringing.
- A blinking LED indicates that the monitored extension has a call on hold, or the extension is in Do Not Disturb mode.

You can include multiple DSS/BLF buttons on a phone.

Phone type: Digital.

Required settings:

- **Extension**. Any valid extension number.

Optional settings:

- **Blind transfer**. If checked, transfers a call without first connecting the user to the recipient to announce the call. Transfers initiated using a feature button with this option enabled will be completed as soon as the target phone rings. When this option is disabled, a consultation transfer (where the user announces the call to the recipient) is performed instead.

Important notes:

- By default the DSS/BLF feature button only reflects the state of the assigned extension's primary line. You can enable a system-wide option (via the General Settings applet) so that a DSS/BLF feature button on a user's digital phone reflects the assigned extension's state for any line, not just the extension's primary line. For example, if the user at extension 201 is busy on an Outside Line or on a line appearance, another user with a DSS/BLF feature button assigned to extension 201 will see that the user is busy on a call. For more information, see "Enabling DSS/BLF updates when the user's phone is active on any line" on page 16-29.

- You cannot create a DSS/BLF feature button on a phone and assign it that phone's extension. If in a user template you create a new DSS/BLF feature button or change the extension associated with an existing DSS/BLF feature button and then apply that template, the new DSS/BLF feature button extension assignment will be reflected on all users' digital phones that are associated with that user template *except* for a phone with that same extension. The current feature button on that phone will remain unchanged.

Best practice recommendations:

The following feature buttons should be mutually exclusive—there is no functional reason to configure the following buttons with the same extension setting on the same phone:

- Primary
- Line Appearance
- DSS/BLF

For example, having a Primary button with extension 201, and a Line Appearance button for 201, and/or a DSS/BLF button for 201 will result in multiple updates to the phone. These updates may confuse users when multiple buttons light up when they use their phones, and may cause other unintended consequences.

Directed Park feature

Parks a call on a specific extension number. You can include multiple Directed Park buttons on a phone. Directed Park buttons on different phones, targeted to the same extension, are also supported.

Phone type: Digital, SIP.

Required settings: None.

Optional settings:

- **Extension**. Any valid extension number. If you do not enter an extension here, after pressing the Directed Park button the user must enter the extension number on which to park the call, followed by #.
- **Display Status**. If checked, enables the Directed Park LED on the phone to indicate the state of a parked call, and simplifies unparking the call by recalling the extension number on which the call was parked.

Do Not Disturb feature

Enables the user to toggle between Do Not Disturb mode and normal phone operation. Do Not Disturb Mode prevents a user’s phone from ringing, and also blocks pages and voice calls to the user's phone. If the user is a member of a station hunt group, only the user's phone is affected. You can include one Do Not Disturb button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Extension Pickup feature

Answers a specific ringing primary or secondary line within a call pickup group. You can include one Extension Pickup button per phone. See “Configuring call pickup groups” on page 16-5 for more information about configuring call pickup groups.

Phone type: Digital.

Required settings: None.

Optional settings:

- **Extension**. Any valid extension number within the Primary extension number’s call pickup group.

Flash feature

Allows a user to utilize many of the phone’s features (for example, making and transferring calls, placing calls on hold, and so forth.) It is also used with many of the phone feature codes (for example, Flash + *54). You can include one Flash button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Group Pickup feature

Answers any ringing phone within your call pickup group. You can include one Group Pickup button per phone. See “Configuring call pickup groups” on page 16-5 for more information about configuring call pickup groups.

Phone type: Digital, SIP.

Required settings: None.

Optional settings: None.

Headset feature

Toggles the headset off and on when it is plugged into the phone. You can include one Headset button per phone.

Phone type: Digital.

Required settings: None.

Optional settings:

- **Extension**. Not currently used.
- **2.5 mm**. Choose this setting to support a standard headset. (Applies only to Edge 700 digital phones.)
- **Bluetooth**. Choose this setting to support a Bluetooth® wireless headset.

Note: If you do not select either **2.5 mm** or **Bluetooth**, **2.5 mm** is used as the default setting to support a standard headset. If you select **Bluetooth**, but the phone does not support that capability, the standard headset mode (**2.5 mm**) is assumed.

Hold feature

Places a call on hold while the phone goes on-hook, allowing the user to make another call or use other phone features. You can include one Hold button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Line Appearance feature

Line appearance for an extension other than the extension assigned to the Primary line button, allowing the user to answer calls to more than one extension from the same phone. Line Appearance buttons are also used to answer calls on a specific Call Navigator queue.

You can include multiple Line Appearance buttons on a phone.

Phone type: Digital, SIP.

Required settings:

Extension. Any valid extension number. The extension number can be a primary extension on another phone, or a virtual extension. (A virtual extension does not appear as a primary line on another phone—see page 16-38 for information about configuring virtual extensions.)

Optional settings:

- **Do not ring the telephone**. If checked, disables ringing when a call is received on this line appearance. If checked, this setting also disables the **Receive splash ring when off hook** setting (described below) if it is checked.
- **Receive call waiting tone when off hook**. If checked, a beep sounds if the user is off hook and another call arrives on the line. A beep also sounds if an incoming call hangs up or is forwarded before answering.
- **Off-hook audible alert**. If checked, either rings the phone or produces an alert tone (depending on the phone type) when a call comes in on this line appearance if the phone is engaged in an off-hook activity.

- **Receive splash ring when off hook**. If checked, one short ring blip sounds when another call comes in while the user is off hook. Even if checked, this setting may be disabled if **Do not ring the telephone** (described above) is checked.
- **Use Primary Access Profile**. If checked, applies the access profile configured for the Primary extension number associated with this phone in the User Configuration applet, Overview tab.
- **Use Primary Caller ID**. If checked, applies the External Caller ID rules configured for the Primary extension number associated with this phone in the User Configuration applet, Overview tab.
- **Do not allow break-in**. If checked, prevents the line appearance from joining an active call when the shared extension is being used by another call.
- **Automatic Line Selection**. If checked, applies Automatic Line Selection behavior. See “Automatic Line Selection” on page 29-29 for a description of Automatic Line Selection behavior on Line Appearance buttons.
- **Call Navigator Pickup Group 1-6**. Only used if you are using the Wave Call Navigator software add-on in association with the Queue Status feature. This allows this line appearance to be used for answering calls on a specific Call Navigator queue.

  When there is a waiting call in that queue, pressing the Queue Status button automatically connects the call on this line appearance, if it is available. If this line appearance is not available, the queue call is automatically connected on the primary or other available line appearance on this phone that is also associated with the same Call Navigator Pickup Group. (You do not need to press the associated Primary or Line Appearance button to take the call.)

  Note that a Call Navigator Pickup Group is only used here to associate this Line Appearance button with a Queue Status button. A Call Navigator Pickup Group is not the same as a Wave Pickup Group, and you do not need to create a Wave Pickup Group (as described in “Configuring call pickup groups” on page 16-5) by that name.

  To configure this feature:

  a Select one or more **Call Navigator Pickup Group** checkboxes here to add this line appearance’s extension to the pool(s) of extensions that can answer calls via any associated Queue Status buttons that specify those Call Navigator Pickup Groups.

  Note: A single Queue Status button can specify one or more Call Navigator Pickup Groups to answer calls on the queue that it monitors, and you can define more than one Queue Status button per phone, so this line appearance’s extension may be part of several extension pools.

b Configure a one or more Queue Status buttons that specify the Call Navigator Pickup Group(s) selected.

c Select the **Enable Pickup** checkbox for those buttons.

Important notes:

- **Line Appearance and Call Appearance:** You cannot configure a Line Appearance button mapped to an extension that is already configured as a Call Appearance button on that extension’s primary phone. Similarly, you cannot configure a Call Appearance button on a phone if that phone’s primary extension is already mapped to a Line Appearance button on another phone.

  If either of these configurations are detected when you are editing a user or applying a digital or SIP phone template, Wave displays an error message and does not allow the button to be configured or the template to be applied.

Note: Previous versions of Wave allowed these feature button configurations, and users with the unsupported configurations may still exist in your Wave database. If you are editing one of these users, the unsupported configuration will now prevent the user from being saved even if you made no changes to feature button assignments. If this problem occurs, either remove the Line Appearance button, or remove the Call Appearance button from the primary phone of the extension to which you want to map the Line Appearance button.

Best practice recommendation:

The following feature buttons should be mutually exclusive—there is no functional reason to configure the following buttons with the same extension setting on the same phone:

- Primary
- Line Appearance
- DSS/BLF

For example, having a Primary button with extension 201, and a Line Appearance button for 201, and/or a DSS/BLF button for 201 will result in multiple updates to the phone. These updates may confuse users when multiple buttons light up when they use their phones, and may cause other unintended consequences.

Message Waiting feature

Indicates that a new voicemail message is available in the mailbox. Directly dials the VoiceMail extension number. You can include multiple Message Waiting buttons on a phone.

Phone type: Digital, SIP.

Required settings:

- **Mailbox**. Any valid voice mailbox extension. In order for the Message Waiting LED to light on the phone when a new voicemail message arrives, a valid extension must be configured for the voice mailbox entered in this field. This can be an extension for a physical phone station or a virtual extension.

  If the voice mailbox number does not match the extension number for which this voice mailbox was configured, your Message Waiting buttons will not work.

  To complete the Message Waiting configuration, be sure to set the system VoiceMail extension number in the General Settings applet, System tab, Voicemail System drop-down list.

Optional settings: None.

Mute feature

Toggles the phone's handset microphone or speakerphone off and on. When muted, any distant parties on a call are prevented from hearing anything at the user's end. You can include one Mute button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Night Answer feature

Places the phone into a mode where inbound calls are redirected to predetermined destination. You can configure any on- or off-premise phone number as the destination. See “Configuring Night Answer” on page 16-31 for information about configuring the Night Answer system.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Outside Line feature

A button used for receiving and placing calls on a specific trunk or set of trunks. This allows users to make external calls without having to dial an access code (typically **9**). See “About creating outside lines” on page 5-2 for more information. You can include multiple Outside Line buttons on a phone.

Note: You must first create a trunk group with outside lines enabled (via the Trunks Group applet) before the Outside Line option will be presented in the list of features that can be configured for a digital phone.

Phone type: Digital.

Required settings:

- **Outside Line**. Any trunk group with outside lines enabled via the Trunk Groups applet.

Optional settings:

- **Do not allow break-in**. If checked, denies break-in on any calls on this Outside Line button. This does not affect instances of the outside line on other phones. This setting applies only to Single Call variant outside lines only.
- **Off-hook audible alert**. If checked, an audible tone alerts the user when a call comes in on this line appearance and the phone is off-hook.

- **Automatic Line Selection**. If checked, applies Automatic Line Selection behavior. This setting allows an outside line to be selected for making calls automatically when an external access digit is dialed, or for answering calls automatically when the phone goes off-hook.

  See “Automatic Line Selection” on page 29-29 for a description of Automatic Line Selection behavior on Outside Line buttons.

- **Do not ring the telephone**. If checked, ringing is disabled when a call is received on this line, similar to setting Do Not Disturb for this outside line. When a call comes in, the phone will not ring, but the LED will flash.

Page feature

Accesses the public address system and all the digital phone speakers on your system. Pages can be sent to the entire system or only to specific zones. You can include multiple Page buttons on a phone. See “Configuring zone paging groups” on page 16-39 for information about configuring zone paging groups.

Phone type: Digital, SIP.

Required settings:

- **Zone Paging Group**. Select a paging zone (for example, **01 - Sales**), or select **System Page** to page the entire system.

Optional settings: None.

Primary feature

Primary line appearance. This is the main extension number associated with this phone. You can include only one Primary button per phone.

Phone type: Digital, SIP.

Required settings:

- **Extension**. Any valid extension number.

Optional settings:

- **Do not ring the telephone**. If checked, disables ringing when a call is received on this line appearance. If checked, this setting also disables the **Receive splash ring when off hook** setting (described below) if it is checked.
- **Receive call waiting tone when off hook**. If checked, a beep sounds if the user is off hook and another call arrives on the line. A beep also sounds if an incoming call hangs up or is forwarded before answering.
- **Always select first**. If checked, automatically selects the primary line first when answering a ringing line or going off-hook, regardless of where the Primary button appears on the phone.
- **Receive splash ring when off hook**. If checked, one short ring blip sounds when another call comes in while the user is off hook. Even if checked, this setting may be disabled if **Do not ring the telephone** (described above) is checked.
- **Mute the microphone when voice calls are received**. If checked, prevents the calling party from hearing you when a voice call is placed to this extension number.
- **Off-hook audible alert**. If checked, produces an alert tone when a call comes in on this line appearance if the phone is engaged in an off-hook activity.
- **Do not receive system paging**. If checked, prevents this phone from receiving pages broadcast to the entire system with the Page button. Note that this option does not prevent the phone from receiving a zone-specific (non-system) page.
- **Do not allow break-in**. If checked, prevents the line appearance from joining an active call when the shared extension is being used by another call.
- **Disable paging alert tone**. If checked, disables the paging alert tone on this phone, but allows the phone to receive the page.
- **Auto Privacy.** If checked, all calls answered or placed via this button are private. A private call cannot be broken into by another user's secondary line appearance even if the secondary line appearance is configured to allow break-in. Also, if you put a private call on hold, only the phone used to put the call on hold can retrieve the call.

- **Call Navigator Pickup Group 1-6**. Only used if you are using the Wave Call Navigator software add-on in association with the Queue Status feature. This allows the primary line appearance to be used for answering calls on a specific Call Navigator queue.

  When there is a waiting call in that queue, pressing the Queue Status button automatically connects the call on the primary line appearance, if it is available. If the primary line appearance is not available, the queue call is automatically connected on another available line appearance on this phone that is also associated with the same Call Navigator Pickup Group. (You do not need to press the associated Primary or Line Appearance button to take the call.)

  To configure this feature

  a Select one or more **Call Navigator Pickup Group** checkboxes here to add this line appearance's extension to the pool(s) of extensions that can answer calls via any associated Queue Status buttons that specify those Call Navigator Pickup Groups.

  Note: A single Queue Status button can specify one or more Call Navigator Pickup Groups to answer calls on the queue that it monitors, and you can define more than one Queue Status button per phone, so this line appearance's extension may be part of several extension pools.

  b Configure a one or more Queue Status buttons that specify the Call Navigator Pickup Group(s) selected.

  c Select the **Enable Pickup** checkbox for those buttons.

  Note: A Call Navigator Pickup Group is only used here to associate this Primary button with a Queue Status button. You do not need to create a Wave Pickup Group (as described in "Configuring call pickup groups" on page 16-5) by that name.

Best practice recommendation:

The following feature buttons should be mutually exclusive—there is no functional reason to configure the following buttons with the same extension setting on the same phone:

- Primary
- Line Appearance
- DSS/BLF

For example, having a Primary button with extension 201, and a Line Appearance button for 201, and/or a DSS/BLF button for 201 will result in multiple updates to the phone. These updates may confuse users when multiple buttons light up when they use their phones, and may cause other unintended consequences.

Privacy feature

Marks the call as private. Privacy prevents shared line appearances from breaking into the conversation. Held private calls cannot be retrieved by a shared line. Privacy is extended from any privacy-enabled phone to all parties on a call.

Note: Transferring or parking a call removes the Privacy feature.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Program feature

Programs programmable buttons, such as Auto Dial, User Forward, and Voice Call buttons, and displays information about buttons. You can include one Program button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Queue Status feature

Note: This feature is only used with the Wave Call Navigator software add-on. If you are not using Call Navigator, you do not need to configure a Queue Status button. For more about Call Navigator, see the *Wave Call Navigator Administrator Guide*.

The Queue Status feature indicates whether there are calls in the Call Navigator queue, and answers a call in a queue, if the queue is a Pickup type.

The phone’s LED displays the queue status as follows:

- Off = No calls in queue.
- Flashing slowly = Number of calls in the queue is less than the threshold set in Queue Configuration.
- Faster flashing = Number of calls in the queue is equal to or greater than the threshold set in Queue Configuration.

Phone type: Digital.

Required settings:

- **Queue**. Name of the Call Navigator queue associated with this button.

Optional settings:

- **Enable Pickup**. If selected, when this button flashes (indicating that there are calls in the queue), pressing the Queue Status button dials the pickup code for that queue to take a call. Select this checkbox for a Pickup type queue, or when associating a Queue Status button with a Line Appearance button as described in **Call Navigator Pickup Group**, below.

  If not selected, the button flashes but no pickup is available. Deselect this checkbox for a non-Pickup type queue.

- **Call Navigator Pickup Group 1-6**. Only used in association with the Primary and/or Line Appearance features. This allows a line appearance button to be used for answering calls on a specific Call Navigator queue.

  When there is a waiting call in that queue, pressing the Queue Status button automatically connects the call on the primary or other available line appearance on this phone that is also associated with the same Call Navigator Pickup Group. (You do not need to press the associated Primary or Line Appearance button to take the call.)

To configure this feature:

a Select one or more **Call Navigator Pickup Group** checkboxes here.

b Select the **Enable Pickup** checkbox.

c Configure a Primary button or one or more Line Appearance buttons to use the same Call Navigator Pickup Groups. Those line appearance extensions are then added to the pool(s) of extensions that can answer calls via any associated Queue Status buttons that specify those Call Navigator Pickup Groups.

Note: A Call Navigator Pickup Group is only used here to associate this Queue Status button with one or more line appearance buttons. You do not need to create a Wave Pickup Group (as described in "Configuring call pickup groups" on page 16-5) with that name.

Redial feature

Dials the last dialed phone number. You can include one Redial button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Release feature

Disconnects an active call, clears the phone's display, mutes the speaker during a page, and cancels transfers, conference calls, and the Program feature. You can include one Release button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Restrict feature

Blocks the user’s Caller ID from being displayed to the distant party (the user’s Caller ID will be displayed as “Private”.) This feature only applies to the current call—it must be enabled on a call-by-call basis.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Save/Repeat feature

Allows a user to temporarily store a dialed number while hearing ringback or while connected on a call, and then redial the saved number later.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Self Park feature

Places a call in a parked state on a user’s primary line appearance for retrieval from another phone (using a Directed Park button on the other phone). You can include one Self Park button per phone.

In the General Setting applet, PBX (Advanced) tab, in the Call Park group box, you can specify the Self park **n** minutes before ring back setting. In the Self park drop-down list, select the number of minutes that Wave waits for a user to pick up a self-parked call. If the call is not picked up within the specified time, Wave rings the extension at which the call was parked. If you specify unlimited minutes, then Wave does not ring back the extension.

Phone type: Digital, SIP.

Required settings: None.

Optional settings: None.

Shift feature

Allows a second set of features to be assigned to the programmable buttons on the phone. The additional buttons are activated when the button is pressed while holding down the Shift button.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Important notes:

- Currently, only the Auto Dial feature can be assigned to a shifted button.

Silent Monitor feature

Allows a supervisor to monitor a call between two users. The supervisor can hear the conversation, but cannot be heard by either user. You can include one Silent Monitor button per phone.

Note: In order for this feature to work as expected, the supervisor must have the permission **Can monitor user calls** (see “The Security \ Permissions tab” on page 11-96), and each user must have the permission **Personal calls can be monitored** (see “Configuring whether the user’s calls can be supervised” on page 11-95.)

Phone type: Digital.

Required settings: None.

Optional settings: None.

Speaker feature

Enables the user to toggle between using the speaker and the handset. You can include one Speaker button per phone.

Phone type: Digital.

Required settings: None.

Optional settings: None.

System Speed Dial feature

Enables the automatic dialing of pre-configured speed dial index numbers. You can include multiple System Speed Dial buttons on a phone.

See “Configuring System Speed Dial” on page 16-33 for information on how to configure system speed dial index numbers.

Phone type: Digital, SIP.

Required settings: None.

Note: If neither of the following optional settings are selected, the user is prompted to enter a specific speed dial index number when the button is pressed, and then a call is placed to that number.

Optional settings:

- **Speed Dial Index**. Enter one of the following:
    - A specific speed dial index number, for example **100**.
    - The first one or two digits of an index number range, requiring the user to only enter the remaining digit(s) in order to dial the number. (A speed dial index number can be 1-3 digits.)

      For example, if you have set up system speed dial index numbers 100-199, entering **1** here means the user only has to enter the final 2 digits (such as **99**) in order to dial the number.

- **Preview**. If checked, displays a list of all available speed dial index numbers when the button is pressed.
    - If **Preview** is selected and **Speed Dial Index** is not blank, the number about to be dialed is displayed on the phone. The user can press the button again to dial the number, or scroll through the list of numbers using the volume up and down buttons in order to select a different number (by pressing the button again.)
    - If **Preview** is selected and **Speed Dial Index** is blank, the list of all available speed dial index numbers is displayed, starting with the last number viewed. The user can scroll through the list of numbers using the volume up and down buttons in order to select a different number (by pressing the button again.)

  If **Preview** is not selected, the associated **Speed Dial Index** number is automatically dialed when the button is pressed. If **Speed Dial Index** is blank, the user is prompted to enter a specific speed dial index number which is then dialed.

System Park feature

Places a call in the first available of 10 parking slots for retrieval from another phone. You can include one System Park button per phone.

Phone type: Digital, SIP.

Required settings: None.

Optional settings: None.

Important notes:

- In the General Setting applet, PBX (Advanced) tab, in the Call Park group box, you can specify the **System park n minutes before ring back** setting. In the System Park drop-down list, **n** is the number of minutes that Wave waits for a user to pick up a parked call. If the call is not picked up within the specified time, Wave rings the extension from which the call was parked. If you specify unlimited minutes, Wave does not ring back the parking extension.

Tap feature

Does the following:

- Retrieves a call that was placed on hold using the HOLD button.
- Places an active call on hold and gets dialtone.
- Toggles between a call on hold and an active call.
- While dialing a number, pressing this button once erases the last dialed digit and pressing it twice (within 500 ms) clears all of the dialed digits.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Transfer feature

Transfers calls to another extension. You can include multiple Transfer buttons on a phone.

Phone type: Digital.

Required settings: None.

Optional settings:

- **Telephone Number**. Transfers the call to the specified extension.
- **Blind transfer**. If checked, transfers a call without first connecting the user to the recipient to announce the call.
- **Direct Transfer to Voice Mail**. If checked, transfers a call directly to the specified voice mailbox extension specified in **Telephone Number**. This option generates a phone button label called **Transfer VM**. You must specify the VoiceMail hunt group extension in **Telephone Number** if you select this setting.

TRNS/CONF feature

Initiates either a conference or transfer. Pressing the TRNS/CONF button puts the current call on hold while the call is transferred or while other members are added to a conference call. The user may then do one of the following:

- Press TRNS/CONF a second time to conference the new call to the call on hold.
- Press Transfer (or SPEAKER, or hang up) to transfer the call on hold.
- Press Release or the Line Appearance button to drop the new call and return to the call on hold.
- Press TAP to toggle between the two calls.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Unassigned feature

No feature is assigned to the button. You can include multiple Unassigned buttons on a phone.

Phone type: Digital, SIP.

Required settings: None.

Optional settings: None.

User Forward feature

Forwards calls to another extension or phone number. You can include multiple User Forward buttons on a phone.

When forwarding to an external number, you must enter the number exactly as you would dial it using the phone, including the first digit (for example 9).

Phone type: Digital.

Required settings: None.

Optional settings:

- **Telephone Number**. Forwards the call to the specified extension. If you leave this field blank, the user can program a number from the phone.

Important notes:

- Configure the following call forwarding-related options in the General Setting applet, PBX (Advanced) tab, in the Trunking group box:
  - **Off-Site Call Forward Password Required**. If checked, users must enter their voicemail passwords when forwarding their phone calls to an external number.

    If you select this option, users must enter their voicemail password after specifying the external number when they dial *43 (or press the Forward button on a digital phone) to forward their calls to an off-site number.

    Note that users without passwords can use the password **111** when prompted to forward calls to an external number.

Caution! *It is strongly suggested that you configure passwords for all users. Password security is crucial in preventing your company from being victimized by toll fraud, where unauthorized users gain privileged access to your telephone system and place outbound long distance or international calls that are then charged to you. In most cases, access is gained through unsecure, easy-to-guess passwords. By making your passwords more secure, you can dramatically increase the security of your Wave system against toll fraud. For more information, see Appendix Appendix A.*

  - **Allow External Trunk-to-Trunk Connections.** If checked, enables external trunk-to-trunk connections. In this scenario, a call is physically connected across two external trunks through Wave. If you enable external trunk-to-trunk connections, Wave allows calls to be forwarded, transferred, and conferenced between external numbers.

- The following behavior, which occurs on all digital phone models, may be confusing to users:

  - **If a user *does not* have a forwarding number set up via the User/Group Management applet** (User dialog, Phone \ Call Handling tab), when that user presses the User Forward button on his or her digital phone and enters a forwarding number, the button’s LED flashes red until the user presses the User Forward button again to cancel call forwarding.

  - **If a user *does* have a forwarding number set up via the User/Group Management applet**, the user may observe either of the following:

    When that user presses the User Forward button on his or her phone and enters a forwarding number that *matches* the number set up set up via the User/Group Management applet, the button’s LED displays solid red until the user presses the User Forward button again to cancel call forwarding.

    When that user presses the User Forward button on his or her phone to enter a forwarding number that is *different* from the number set up via the User/Group Management applet, the button’s LED remains off.

Voice Call feature

Directs an intercom page to a specific digital or SIP phone extension. You can include multiple Voice Call feature buttons on a phone.

Phone type: Digital, SIP.

Required settings: None.

Optional settings:

- **Extension**. Any valid extension number. If you leave this field blank, the user can program the button or dial an extension from the phone.

Important note:

If you configure Voice Call feature buttons on users' digital or SIP phones, be sure that those users understand the following behavior:

- A digital or SIP phone user making a voice call may assume that only the called extension will receive the voice call. Note that in Wave, a voice call may be forwarded to another user's extension or to the company operator, or be transferred as a voice call if the call happens to reach the company Auto Attendant or dial-by-name directory.
- A voice call to a phone that has a call on hold (even if there are available lines on that phone) will be automatically forwarded to that extension's If Busy call forwarding setting, which may be any of the targets listed above.

The result of this behavior may be unexpected or problematic for a user who did not expect the voice call to reach someone he or she didn't voice call directly, as well as for a user who receives unexpected voice calls.

Volume Reset Override feature

Allows the user to override the automatic reset of the handset/headset volume, and retain the previous setting.

Note: This feature is sometimes called “Volume Ring Override”.

Phone type: Digital.

Required settings: None.

Optional settings: None.

Wave Phonebook feature

The Wave Phonebook is a searchable directory of public ViewPoint Groups or private contacts that is accessible directly from a button on a user's Edge 5000i IP phone. Especially for users with no access to ViewPoint, this feature provides access to the same synchronized directory information as other Wave users have, and makes deploying custom phonebooks (for example customer contact directories) easy to deploy.

- See "The Phone \ Wave Phonebook tab" on page 11-86 for more about how to set up a Wave Phonebook for a user.
- See the *Wave Phone User Guide* for information about how to use the Wave Phonebook on and Edge 5000i IP phone.

Phone type: SIP—Edge 5000i IP phones only.

Required settings: None.

Optional settings: None.

Configuring hunt groups of extensions

You create a station hunt group of user extensions when you want to have phone calls routed to a group of users.

- **Station hunt groups** are used to route calls to groups of extensions. Note that calls to a station hunt group do not follow a user's external call forwarding setting. If a user is a member of a hunt group and that user has forwarded calls to an external number, calls to the hunt group that are sent to that user are not forwarded to the external number as expected. Instead, calls are forwarded to the hunt group’s **When busy, forward to extension** ___ setting (specified in the Station Hunt Group dialog.)
- The **Attendant hunt group** is a station hunt group that is used by the Attendant digit (default=0) for dialing the company operator, and it is used to forward inbound calls to the company operator or Auto Attendant. Attendant hunt group search order is based on the number of calls being handled by a member, not the number of available lines on a member’s phones. Also, the Attendant hunt group rings all available members of the group for a call before repeating any members.

  Specifically, the Attendant hunt group assigns calls in a fashion similar to a hunt group with a Circular hunt order, unless some of the stations are already handling other calls. In that case, the call will be assigned to the member currently handling the fewest number of calls, provided that member has the capacity to accept another call. If a member is in Do Not Disturb mode or is already handling calls on all available lines, then the unanswered call will continue to the next member that hasn’t yet been offered the call. Once the call has been offered to all available members of the group, the unanswered call may then re-ring a member who was previously offered the call, until the call has rung the programmed number of members before forwarding.

  Deleting the default Attendant Hunt Group x0 (Operator) removes this default operator as the personal operator of any users to which it is assigned, so you will need to reassign the hunt group (or another extension) as the personal operator for those users. New users will be set to use the hunt group as personal operator by default, if it exists.

This section describes how to do the following:

- Configuring the Attendant hunt group. See page 10-44.
- Creating a station hunt group. See page 10-48.
- Adding members to hunt groups. See page 10-50.
- Deleting a hunt group. See page 10-51.

Configuring the Attendant hunt group

Configuring the Attendant consists of the following:

- **Specifying an Attendant digit via the First Digit Table applet.** Any digit—but only one—can be configured as the Attendant digit in the First Digit Table applet. If the Attendant digit is changed from the default of 0, the Attendant hunt group pilot number must also be changed, to ensure that the company operator and Auto Attendant will receive all calls routed to the attendant. Note that the 0 digit can be configured in the First Digit Table as Not Configured, Attendant, or External, but it cannot be configured for Extension.

  Note: If you change the default Attendant digit, be careful not to introduce a dialing conflict by selecting a new Attendant digit (for example 9) that matches the first digit of your emergency number (for example 911). This configuration will prevent extensions in the Attendant hunt group from ringing as expected. To avoid this problem, do either of the following:

  - Do not configure the Attendant digit to match the first digit of your emergency number.
  - In the General Settings applet, on the PBX (Advanced) tab, select the **Require external access code** to dial emergency numbers checkbox to resolve the dialing conflict. See “Requiring an access code for emergency number dialing” on page 16-13 for more information.

- **Assigning extensions to the Attendant hunt group via the Hunt Groups applet**. Hunt group members with the Attendant hunt order are typically stations that can handle multiple calls simultaneously. The Attendant hunt order is valid for station hunt groups only.

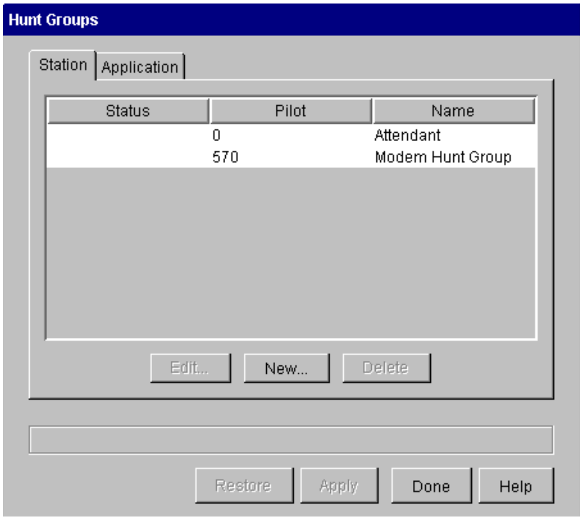
  The Attendant hunt group assigns calls in a fashion similar to a hunt group with a Circular hunt order, unless some of the stations are already handling other calls. In that case, the call will be assigned to the member currently handling the fewest number of calls, provided that member has the capacity to accept another call. If a member is in Do Not Disturb mode or is already handling calls on all available lines, then the unanswered call will continue to the next member that hasn’t yet been offered the call. Once the call has been offered to all available members of the group, the unanswered call may then re-ring a member who was previously offered the call, until the call has rung the programmed number of members before forwarding.

To configure the Attendant hunt group:

1 If necessary, click the Administration tab of the Management Console.

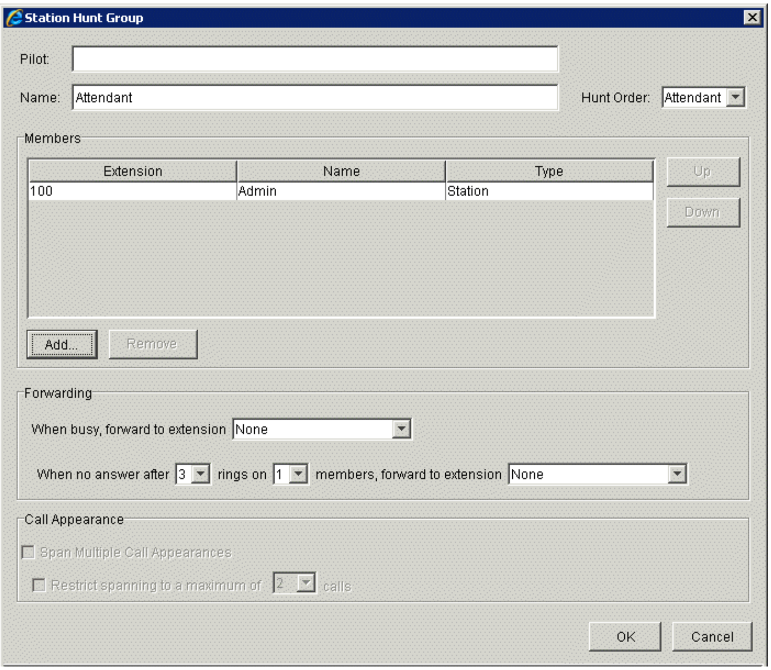
Click

2 Click the Hunt Groups icon, located in the PBX Administration section.



Status	Pilot	Name
	0	Attendant
	570	Modem Hunt Group

3 Select the Attendant hunt group from the Station tab, and then click **Edit**. The Station Hunt Group dialog opens.



Station Hunt Group

Pilot:

Name: Attendant

Hunt Order: Attendant

Members

Extension	Name	Type
100	Admin	Station

Forwarding

When busy, forward to extension None

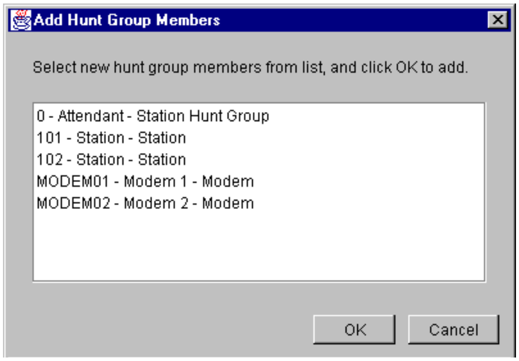
When no answer after 3 rings on 1 members, forward to extension None

Call Appearance

□ Span Multiple Call Appearances

□ Restrict spanning to a maximum of 2 calls

4 Click **Add** to open the Add Hunt Group Members dialog.



Add Hunt Group Members

Select new hunt group members from list, and click OK to add.

0 - Attendant - Station Hunt Group
101 - Station - Station
102 - Station - Station
MODEM01 - Modem 1 - Modem
MODEM02 - Modem 2 - Modem

5 Select the members you wish to add, and click **OK**.

Use Ctrl-click or Shift-click to select multiple extensions. A maximum of 64 extensions can be in a single hunt group.

6 In the Forwarding section, specify the forwarding destinations for calls that come into the Attendant hunt group when all the extensions included in the hunt group are busy or do not answer. Note that if you do not select a busy forward destination, callers will hear a busy tone.

- **When busy, forward to extension**. Specify the extension to which the calls will be forwarded when all of the hunt group member extensions are busy. The default forwarding destination for the Attendant hunt group is the VoiceMail hunt group pilot number, which allow the caller to leave a message.
- **When no answer**. Use the following fields to specify how unanswered calls will be handled.
  - **after ___ rings**. Specify the number of rings before forwarding. If a call is not answered at an extension after the ring count elapses, it will be forwarded to the next member of the hunt group.
  - **on ___ members**. Specify the number of stations in the hunt group to be rung in succession. For example, if there are five hunt group members and the number of stations is set to three, only three of the five members will be rung before a call is forwarded to the no-answer destination.
  - **forward to extension**. Specify the extension (user, hunt group, or voicemail) to which calls will be forwarded when none of the hunt group member extensions answer.

    Keep in mind that a ring cycle is six seconds long—two seconds of ringing and four seconds of silence. Avoid configuring the hunt group for too many rings or too many members to ring or the caller will hear only ringing for an extended period and may hang up.

Note: When a call is initially placed to a hunt group pilot number, the ring count specified above supersedes the **Ring Phone X Times** count configured in the Phone tab of the User dialog, for extensions in that hunt group.

7 Click **OK** to close the Station Hunt Group dialog, and return to the Management Console.

Creating a station hunt group

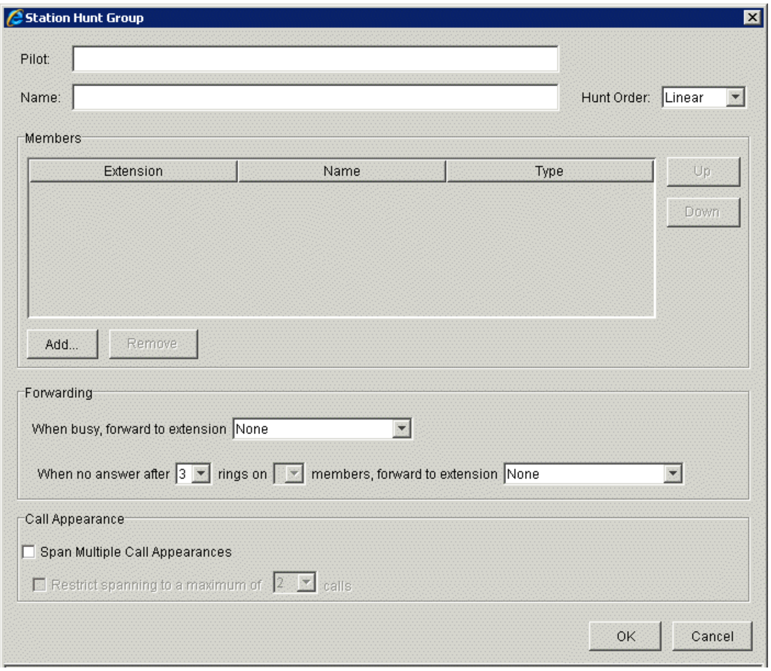
To create a new station hunt group

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Hunt Groups icon, located in the PBX Administration section.

3 Click **New** in the Station tab of the Hunt Groups applet. The Station Hunt Group dialog opens.



Station Hunt Group

Pilot:

Name:

Hunt Order: Linear

Members

Extension	Name	Type

Up
Down
Add...
Remove

Forwarding

When busy, forward to extension None

When no answer after 3 rings on members, forward to extension None

Call Appearance

□ Span Multiple Call Appearances

□ Restrict spanning to a maximum of 2 calls

OK Cancel

4 Enter a unique **Pilot** number for the hunt group. A pilot number is the number users dial, or trunk groups use, to reach the members of a hunt group.

The pilot number is similar to an extension:

- It must be unique
- It must fit into your first digit dialing plan for internal numbers
- It must comply with the Internal extension length setting in the First Digit Table

5 Enter a **Name** for the hunt group. You can enter up to 16 alphanumeric characters in the **Name** field.

6 Select the desired hunting method from the **Hunt Order** drop-down list.

You have four hunt order options: Linear, Circular, Ring, and Attendant. For descriptions, see “Hunt group hunt orders” on page 29-25.

7 In the Forwarding section, specify the forwarding destinations for calls that come into the Attendant hunt group when all the extensions included in the hunt group are busy or do not answer. Note that if you do not select a busy forward destination, callers will hear a busy tone.

- **When busy, forward to extension**. Specify the extension to which the calls will be forwarded when all of the hunt group member extensions are busy. The default forwarding destination for the Attendant hunt group is the VoiceMail hunt group pilot number, which allow the caller to leave a message.
- **When no answer.** Use the following fields to specify how unanswered calls will be handled.
  - **after ___ rings**. Specify the number of rings before forwarding. If a call is not answered at an extension after the ring count elapses, it will be forwarded to the next member of the hunt group.
  - **on ___ members**. Specify the number of stations in the hunt group to be rung in succession. For example, if there are five hunt group members and the number of stations is set to three, only three of the five members will be rung before a call is forwarded to the no-answer destination.
  - **forward to extension**. Specify the extension (user, hunt group, or voicemail) to which calls will be forwarded when none of the hunt group member extensions answer.

    Keep in mind that a ring cycle is six seconds long—two seconds of ringing and four seconds of silence. Avoid configuring the hunt group for too many rings or too many members to ring or the caller will hear only ringing for an extended period and may hang up.

8 To send multiple hunt group calls to users who have multiple call appearance lines on a digital phone, check **Span multiple call appearances**. Then use the **Restrict spanning to a multiple of __ calls** field to enter the maximum number of calls that can be sent to a single phone.

For example, if you enter a Restrict spanning number of 5, and a phone has 8 call appearance lines, only 5 calls will be sent to the phone.

9 Click **OK** to close the Station Hunt Groups dialog.

The new hunt group is displayed in the list. To add members to the new group, proceed to step 3 in the next section "Adding members to hunt groups."

10 Click **Apply** to save your changes.

11 Click **Done** to return to the Management Console.

Adding members to hunt groups

Member extensions are the extensions that a hunt group rings when the hunt group pilot number is dialed. Once a hunt group is created, member extensions can be added.

Note the following:

- A single hunt group can have a maximum of 64 extensions.
- You cannot add gateway users (users on another Wave Server in a WaveNet network) or remote users to a hunt group.

To add member extensions to a hunt group

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Hunt Groups icon, located in the PBX Administration section.

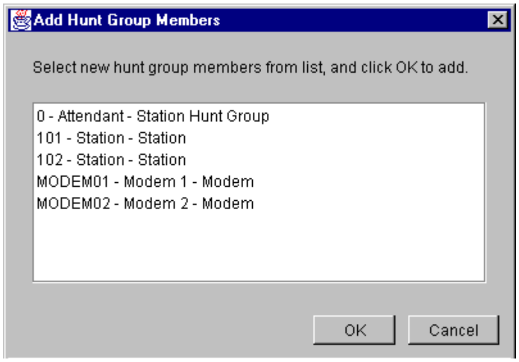
3 Click the Station tab.

4 Select the hunt group to which you want to add members.

5 Click **Edit**.

The Station Hunt Group dialog opens.

6 Click **Add**. The Add Hunt Group Members dialog opens.


Add Hunt Group Members

Select new hunt group members from list, and click OK to add.

0 - Attendant - Station Hunt Group
101 - Station - Station
102 - Station - Station
MODEM01 - Modem 1 - Modem
MODEM02 - Modem 2 - Modem

7 Select the extensions you want to add as members of the hunt group. Use Ctrl-click or Shift-click to select multiple extensions.

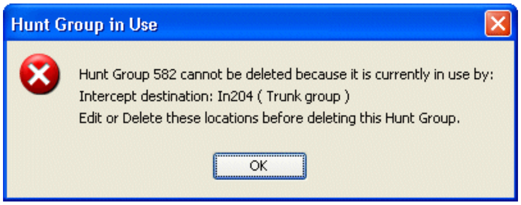
8 Click **OK**. The Add Hunt Group Members dialog closes.

9 Click an extension and use the **Up** and **Down** buttons to rearrange the order of the extensions in the hunt group.

10 Click **OK** to close the Station Hunt Group dialog, and return to the Management Console.

Deleting a hunt group

If you try to delete a hunt group that is in use in other places in Wave, a dialog is displayed that lists these locations.


Hunt Group in Use

Hunt Group 582 cannot be deleted because it is currently in use by:
Intercept destination: In204 (Trunk group)
Edit or Delete these locations before deleting this Hunt Group.

You must modify or delete these locations before you can delete the hunt group.

To delete a hunt group

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Hunt Groups icon, located in the PBX Administration section.

3 Click the hunt group's tab.

4 Select the hunt group and then click **Delete**. If necessary, modify or delete any locations where the hunt group is being used.

5 Click **OK** to close the Station Hunt Group dialog, and return to the Management Console.

Enabling and disabling station ports

The Station Ports applet lets you enable and disable all of the station ports on a card or module, or individual ports.

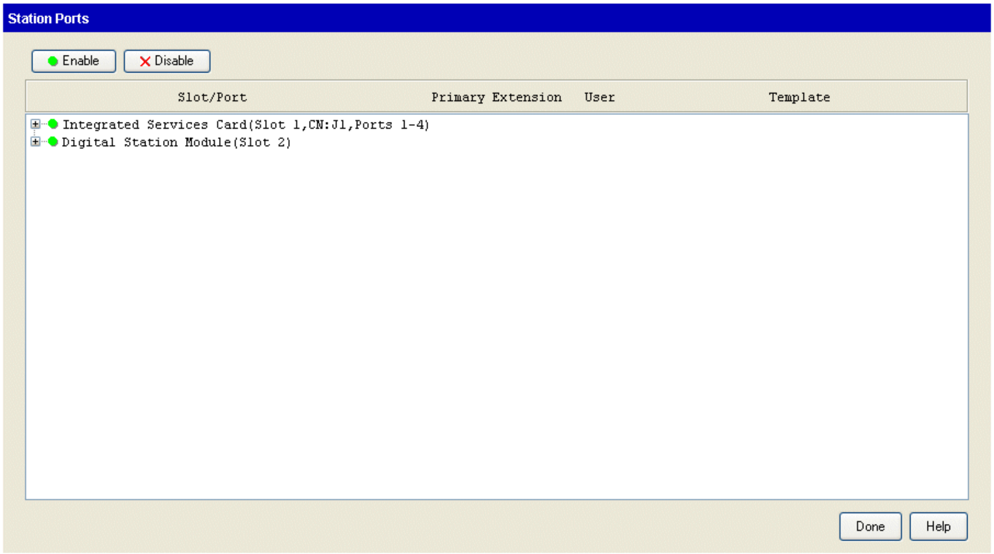
To enable or disable station ports

1 If necessary, click the Administration tab of the Management Console.

Click

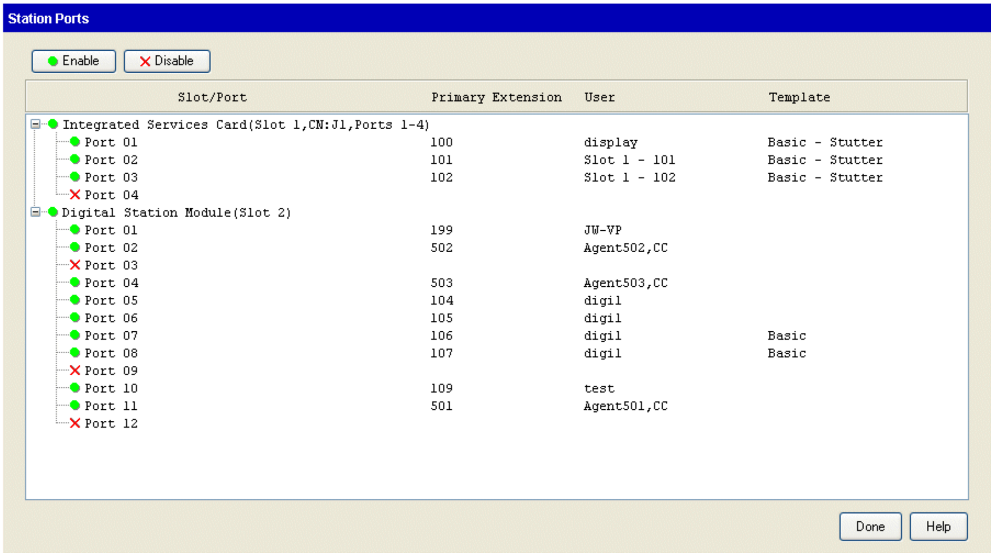
2 Click the Station Ports icon, located in the PBX Administration section.

3 The Station Ports applet opens and displays the cards and modules currently installed in the Wave Server that provide station ports and the status of each one (enabled or disabled).



Slot/Port	Primary Extension	User	Template
⊞ ● Integrated Services Card(Slot 1,CN:J1,Ports 1-4)			
⊞ ● Digital Station Module(Slot 2)			

4 Select a card or module and then use the **Enable** and **Disable** buttons to enable or disable all of he station ports on that card or module. To enable or disable individual ports, expand the card or module first, then select the individual ports you would like to enable or disable. You can use the CTRL or Shift keys to select multiple station ports.



Slot/Port	Primary Extension	User	Template
⊟ ● Integrated Services Card(Slot 1,CN:J1,Ports 1-4)			
● Port 01	100	display	Basic - Stutter
● Port 02	101	Slot 1 - 101	Basic - Stutter
● Port 03	102	Slot 1 - 102	Basic - Stutter
✕ Port 04			
⊟ ● Digital Station Module(Slot 2)			
● Port 01	199	JW-VP	
● Port 02	502	Agent502,CC	
✕ Port 03			
● Port 04	503	Agent503,CC	
● Port 05	104	digil	
● Port 06	105	digil	
● Port 07	106	digil	Basic
● Port 08	107	digil	Basic
✕ Port 09			
● Port 10	109	test	
● Port 11	501	Agent501,CC	
✕ Port 12			

The following information is displayed for each station port:

- **Status (Enabled or Disabled)**
- **Primary Extension.** Primary extension associated with the port.
- **User.** User associated with the port's extension.
- **Template.** Phone template associated with the port's extension.

5 Click **Done** to return to the Management Console.

Chapter 11

Managing Users and Roles

CHAPTER CONTENTS

Unlike a traditional PBX, Wave manages phone traffic by user and role, rather than by device, giving the system the flexibility to handle users who move from phone to phone. Roles are templates of specific permissions that you can use to create categories of users with different permission levels, such as Admin users (see “Managing roles” on page 11-122.)

How to set user options

User options are set in both the User/Group Management applet and ViewPoint.

- **Some options can only be set in the User/Group Management applet.** These options are described in detail in this chapter.
- **Some options can only be set in ViewPoint.** These include the user’s routing lists, contacts, voicemail greetings, call rules, and personal ViewPoint Groups. ViewPoint options are described in detail in *Wave ViewPoint User Guide*.
- **Some options can be set in both places.** You can set up users with standard defaults for your organization and then individual users can override or customize the settings further. You also can restrict the some of options that users can customize.

You can also set user options in bulk via user templates. See “Creating and updating users via a user template” on page 11-107 for more information.

How to add users

You can add Wave users using any of the following methods:

- Adding users via the User dialog. See page 11-107.
- Creating and updating users via a user template. See page 11-107.
- Importing users via a CSV file. See page 11-114.

The Admin user

The Admin user comes pre-defined in Wave, and belongs to the Administrators role. The Admin user and all users who belong to the Administrators role are permitted to run the User/Group Management applet. They also can perform all administrative functions.

You can give individual administrative permissions to any user—for example, permission to shut down the phone system—without making the user a member of the Administrators role. See “Wave permissions” on page 11-127.

Changing the Admin user’s password

Immediately after installing Wave, you should change the passwords of the Admin user and Operator user, in order to make your system more secure from unauthorized access. For more information, see “Changing the Admin and Operator passwords” on page A-3.

Adding users on a Wave IP 500 Server

When you add a user, you specify the type of phone (SIP, digital, or analog) assigned to that user (as described in “Specifying a phone type and model” on page 11-17).

On a Wave IP 500 Server, be aware of the following limits when you add users:

- A maximum of 50 analog, digital, and SIP phones are supported in a mixed configuration.
- A maximum of 50 SIP phones are supported in a SIP-only configuration (with no digital or analog phones)
- A maximum of 48 digital phones are supported in a digital-only configuration (with no SIP endpoints or analog phones)

Increasing the number of digital phone users on a Wave IP 500 Server

The Wave IP 500 requires an external power supply to provide power to digital phones. When you ordered your Wave IP 500, the appropriate model external power supply was included, based on the number of digital phones you planned to support.

- The 120W external power supply supports up to 24 digital phones.
- The 180W external power supply supports up to 48 digital phones.

If you add digital phone users to your Wave Server at a later time, you may need to upgrade the external power supply to avoid any problems. Contact your Wave provider for more information.

Note: In a worst-case scenario—a very heavily-used system with all phones in constant use at full power (all LEDs on, speaker phones on full volume, and so forth), the external power supply could shut down and all digital phones could stop working.

Adding ViewPoint Mobile App users

While the ViewPoint Mobile App is supported on all of Apple's idevices, including the iPhone—iPhone 3GS, iPhone 4, and iPhone 4S—and the iPad and iPod Touch, the available functionality varies. The App allows a user to make and take calls (on the iPhone) and access some ViewPoint features (on the iPhone, iPad, or iPod Touch).

- **iPhone**. iPhone users rely on the iPhone’s built-in voice capability to take and place calls.
- **iPad or iPod Touch**. These users can use the Viewpoint Mobile App to manage personal status, check voicemail, send Instant Messages, see other users’ presence information and personal status, and check their Call Log, but they must use a separate phone to take and place calls since these devices do not have built-in voice capability.

  Important! Although third-party SIP softphones are available for these devices, they are not supported for use with the ViewPoint Mobile App because they can negatively affect battery life.

For details about using the ViewPoint Mobile App, see Chapter 14 in the *Wave ViewPoint User Guide*.

License requirements

In order for users to log in and make and take calls using the ViewPoint Mobile App, you must obtain and activate adequate Wave ISM User licenses. (Each Wave ISM User license is bundled with licenses that allow one user to run both desktop ViewPoint and the ViewPoint Mobile App.) For example, if *n* licenses have been activated, the *n+1* and subsequent users will not be able to log in and connect to Wave, but will be able to see items that are available when the ViewPoint Mobile App is disconnected, such as voice messages, Call Log entries, and contacts.

ViewPoint Mobile App user configuration

To enable a user to use the ViewPoint Mobile App, in the User dialog:

- **Required:** Enable the user permission **Allow ViewPoint Mobile Connection** on the Security / Permissions tab. See “Wave permissions” on page 11-127.
- **Optional (but recommended):** Enable the setting **Imitate a Mobile Extension when routing incoming calls to external numbers** on the Phone tab. This allows the user’s mobile phone to be treated as a Wave station and ensures that calls forwarded to the user’s ViewPoint Mobile extension also appear in the user's Call Log in ViewPoint.
    - **iPhone users**. Configure the iPhone as a Wave mobile extension.
    - **iPad or iPod Touch users**. Configure the user’s associated phone as a Wave mobile extension. (Since these devices do not have voice capability, a separate phone—such as a cell phone—can be used.)

  See “Using mobile extensions for externally routed calls” on page 11-63.

If a user does not have a physical Wave phone

If a user does not have a physical Wave phone (in other words, a phone that rings when a call is received), calls to that user’s extension will automatically be forwarded to voicemail. That user will still be able to answer calls via the ViewPoint Mobile App on his or her mobile device, but the caller will probably already be leaving a message by the time the call is connected. This is similar to the way ViewPoint behaves when a user answers a call in the “Leaving Message” state in ViewPoint Desktop.

Changing the ViewPoint Mobile Port

By default, Wave uses port TCP 50070 to communicate with remote devices using the ViewPoint Mobile App. If this results in a conflict or you want to change the port number for any reason, use the General Settings applet.

You cannot specify the following ports, which are already in use:

21: File Transfer Protocol (FTP)

22: Secure Shell (SSH)

23: Telnet remote login service

25: Simple Mail Transfer Protocol (SMTP)

53: Domain Name Service (DNS)

80: Hypertext Transfer Protocol (HTTP)

110: Post Office Protocol (POP)

119: Network News Transfer Protocol (NNTP)

143: Internet Message Access Protocol (IMAP)

161: Simple Network Management Protocol (SNMP)

443: HTTP Secure (HTTPS)

5222: Wave's own XMPP port

Important! Your firewall must allow outbound connectivity from the Wave Server on the port you specify. Most firewalls allow any outbound port connection, but some do not.

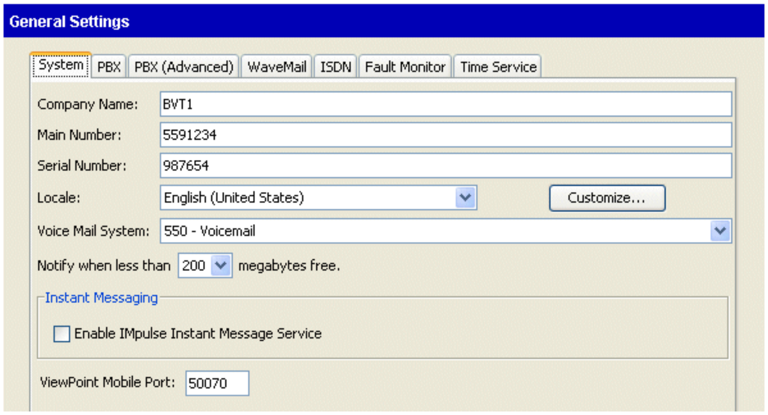
To change the ViewPoint Mobile Port

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Click the System tab.



General Settings

Company Name: BVT1

Main Number: 5591234

Serial Number: 987654

Locale: English (United States)

Voice Mail System: 550 - Voicemail

Notify when less than 200 megabytes free.

Instant Messaging

□ Enable IMpulse Instant Message Service

ViewPoint Mobile Port: 50070

4 In **ViewPoint Mobile Port**, enter the new port to use. You can enter any number from 0 to 65535. You will receive an error message if you specify a port number that is already in use, or if the field is blank. Your firewall must allow outbound connectivity from the Wave Server on the port you specify.

5 Click **Done** to return to the Management Console.

The Users view

You add, edit and delete users in the Users view. To open the Users view:

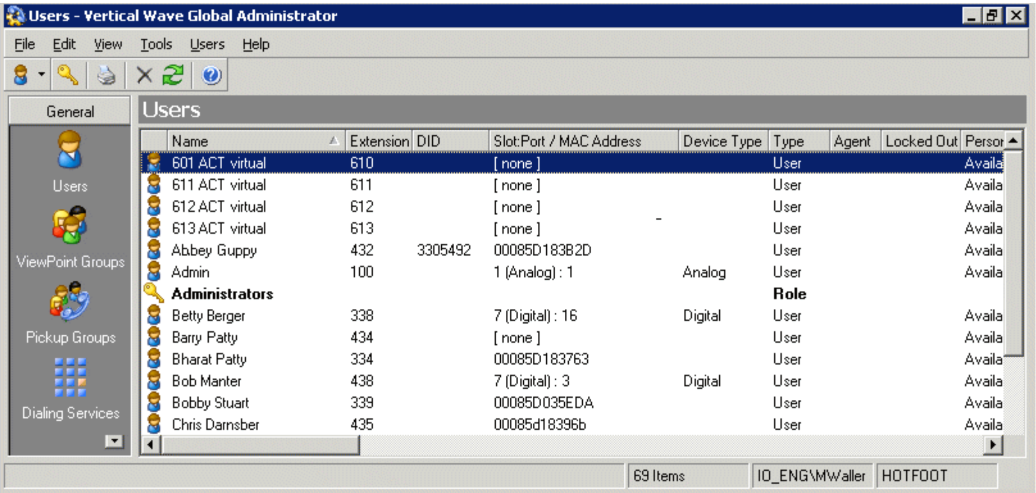
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Log on to the User/Group Management applet, which opens in a remote access window. Once you log on, the Users view opens. See “Accessing the User/Group Management applet” on page 2-15 for more about logging on to the User/Group Management applet.

The Users view presents information about individual users and roles in your organization. Double-click a user in the view to edit that user.



Users

Name	Extension	DID	Slot:Port / MAC Address	Device Type	Type	Agent	Locked Out	Persor
601 ACT virtual	610		[none]		User			Availa
611 ACT virtual	611		[none]		User			Availa
612 ACT virtual	612		[none]		User			Availa
613 ACT virtual	613		[none]		User			Availa
Abbey Guppy	432	3305492	00085D183B2D		User			Availa
Admin	100		1 (Analog) : 1	Analog	User			Availa
Administrators					**Role**			
Betty Berger	338		7 (Digital) : 16	Digital	User			Availa
Barry Patty	434		[none]		User			Availa
Bharat Patty	334		00085D183763		User			Availa
Bob Manter	438		7 (Digital) : 3	Digital	User			Availa
Bobby Stuart	339		00085D035EDA		User			Availa
Chris Darnsber	435		00085d18396b		User			Availa

69 Items | IO_ENG\MWaller | HOTFOOT

Roles appear in bold in the Users view. For more information about roles, see “Managing roles” on page 11-122.

Each user that you add is displayed as a row in the Users view. The following table shows the information that is displayed for each user.

You can sort by the information in any column by clicking the column header. If a column does not appear in your view, it is hidden. To show it, choose **Tools > Columns**. Select the appropriate view, and then check the columns you want to show.

Column	Description
Name	User's name.
Extension	Extension number dialed to reach the user.
DID	*This feature is not supported in this version.*
Slot:Port / Mac Address	Identification of the phone assigned to the user.
Device Type	The type of station, **Analog**, **Digital**, **IP**, or **External**.
Type	The type of user, **User** or **Role** (see "Managing roles" on page 11-122).
Agent	If checked, the user is an agent in one or more Contact Center queues. See the *Wave Contact Center Administrator Guide*.
Must Change Password	If checked the user will be required to change his or her password the next time he or she logs in. Note that this column is checked only if the field **User must change password on next logon** is checked for the user in the User dialog - Security tab. The column is not checked if the user's password has expired.
Password Never Expires	If checked, the user's password never automatically expires according to the system setting for automatic password expiration
Locked Out	If checked, the user is unable to log in to his or her account due to multiple failed attempts to access that account as defined in System Settings (see "Enforcing strong password security" on page 4-14).
Title	User's title or department name.
Organization	The user's Organization, if one has been assigned. You can set up Organizations that represent different companies within your office, and track users' phone calls by Organization for billing or other purposes.
Personal Status	The name of the user's current personal status.
ACD DND	*This feature is not supported in this version.*

Column	Description
Mail Usage	Percentage of allocated voicemail space currently used. For details on how the information in this and the following two columns is calculated, see “Viewing the user’s disk usage” on page 11-93.
Greeting Usage	Percentage of allocated greeting and voice title space currently used.
Disk Usage (MB)	Amount of disk space in megabytes used by the user's voice message, greeting, and voice title files.
Mailbox Size (min)	Total space allocated to the user for voice messages, in minutes.
Greeting Size (min)	Total space allocated to the user for greetings and voice titles, in minutes.
Forwarding To	Number to which the user is currently forwarding calls.
Gateway Name	*This feature is not supported in this version.*
Listed	If checked, the user is listed in the dial-by-name directory.
Voice Title	If checked, the user has a recorded voice title. You can record titles for users on the Recordings tab of the User dialog, or they can record their own.
Announce Callers	*This feature is not supported in this version.*
Exchange Sync	If checked, Wave and Microsoft Exchange voice messages and contacts are synchronized.
Comments	Comments about the user.

Archiving a user’s voicemail and call recordings

You can manually archive a user’s voicemail and call recordings from the Users view. Archiving mailbox recordings can save space on your hard drive, especially if the mailbox contains call recordings. For an overview of mailbox archiving and instructions on setting up automatic archiving, see “Archiving call recordings and voicemail” on page 22-24.

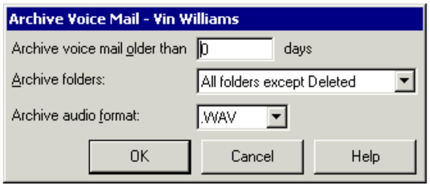
To archive a user’s mailbox recordings from the Users view

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 From the Users view, choose **Users > Archive Mailbox Recordings**. The Archive Voice Mail dialog opens.



Archive Voice Mail - Vin Williams

Archive voice mail older than 0 days

Archive folders: All folders except Deleted

Archive audio format: .WAV

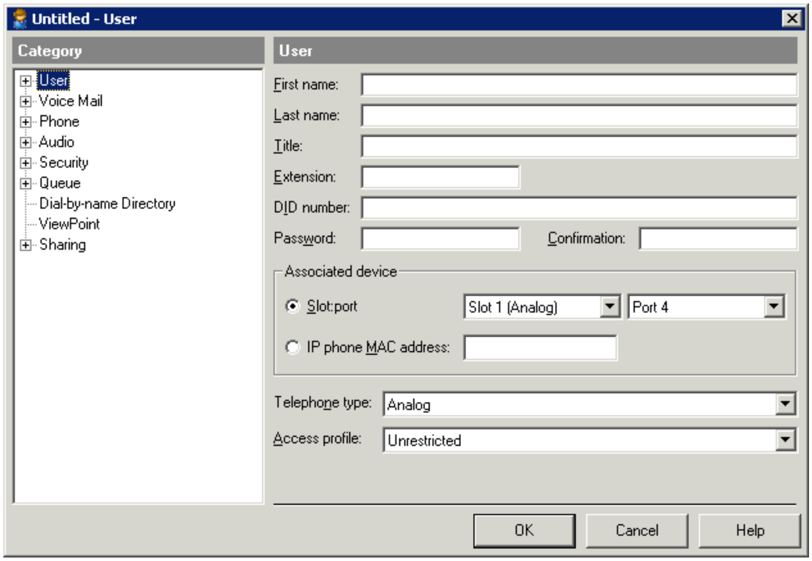
4 Set the following options:

- **Archive voicemail older than __ days**. Enter a number of days. Voicemail older than that will be archived.
- **Archive folders**. Select either **Inbox only** or **All folders except Deleted**.
- **Archive audio format**. Select **WAV** or **MP3**.

5 Click **OK** to archive the user’s mailbox recordings according to the selections made. The recordings are archived in your default archive location (see “Archiving call recordings and voicemail” on page 22-24).

Adding users via the User dialog

To create a new user, in the User/Group Management applet choose **File > New > User**. The User dialog opens.



● Slot:port Slot 1 (Analog) Port 4

Telephone type: Analog

Access profile: Unrestricted

Click in the left pane to select a tab in the User dialog. Click a ⊞ to expand a tab category. Many of the default settings in the User dialog tabs come from the default user template that you specify. For more about user templates, see “Creating and updating users via a user template” on page 11-107.

The following table provides an overview of the tabs, with a cross-reference to more detailed information.

Use this tab	To specify	See page
User	Basic user information, including name, extension, phone type and model, and password. Start here to create a new user.	11-15
User \ Details	Personal operator and other options.	11-19

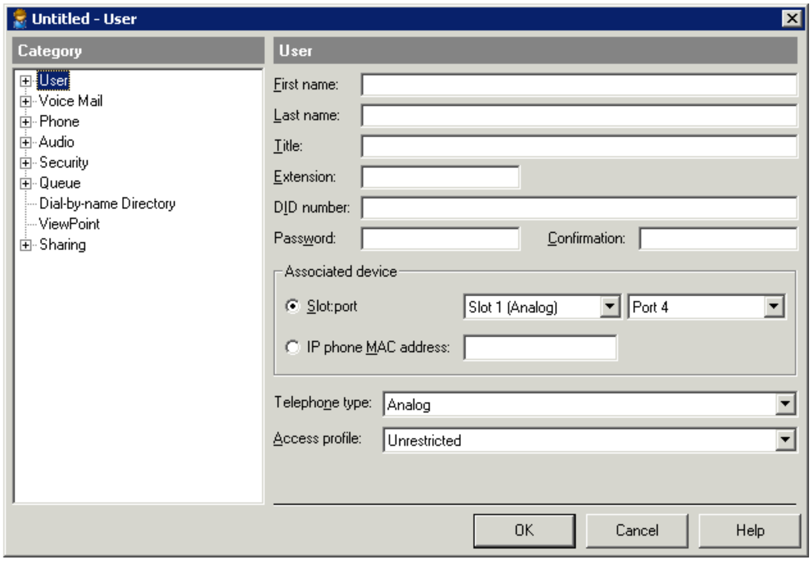
Use this tab	To specify	See page
User \ Account Codes	Whether and under what circumstances Wave prompts the user to enter an account code for a call.	11-21
User \ Call Log	Whether the user’s calls are logged, and whether the user belongs to an Organization.	11-23
User \ External Caller ID	Personalized outbound Caller ID information.	11-25
User \ Numbers	User’s personal numbers.	11-26
Voice Mail	User’s voice mailbox size and features, including configuring WaveMail synchronization settings.	11-28
Voice Mail \ E-Mail Notification, Voice Mail \ Pager Notification, Voice Mail \ Call Notification	Whether and how the user is notified of new voice messages by e-mail, page, or phone call.	11-42
Voice Mail \ Cascading Notifications	Cascading (repeated) notifications if a new voice message is not listened to or acted upon within a specified period of time.	11-54
Phone	Call waiting, Flash behavior, mobile extensions, and other phone options.	11-58
Phone \ Call Handling	Call forwarding, if no answer, and if busy settings.	11-68
Phone \ Station Features	Configure analog, digital, and SIP phone feature buttons. This tab is called Features for an analog phone user.	11-72
Phone \ DSS Consoles	Configure a DSS console device associated with a user’s digital phone to provide additional Line Appearance buttons representing user extensions.	11-74

Use this tab	To specify	See page
Phone \ Ring Patterns	Configurable ring tones for internal and external calls.	11-78
Phone \ SIP	Specify SIP authentication and registration settings for a user.	11-79
Phone \ Softphone	Enable a ViewPoint mobile softphone for the user.	11-81
Phone \ Automatic Log Out	Phone login behavior on other users’ phones.	11-83
Phone \ Networking	Set up OpenVPN Server or NAT traversal for a SIP phone user.	11-85
Phone \ Wave Phonebook	Configure the Edge 5000i Phonebook feature for an Edge IP phone user.	11-86
Audio	Storage size for greeting and voice title files, and phone prompt language.	11-88
Audio \ Hold Music	Personalized hold music source.	11-89
Audio \ Voice Title	The user’s voice title.	11-89
Audio \ Disk Usage	Space usage report for voice messages, greetings, and voice titles.	11-89
Security	Password expiration control, and whether the user’s calls can be supervised.	11-94
Security \ Permissions	All user permissions, and the roles to which the user belongs.	11-96
Queue \ Attributes	Assign non-skill attributes (cost, custom attributes) to the user for call routing purposes.	*Wave Contact Center Administrator Guide*
Queue \ Skills	For skill-based call routing, define a set of skills that you can then assign to the user.	*Wave Contact Center Administrator Guide*
Dial-by-name Directory	Whether the user is listed in the Wave dial-by-name directory.	11-100

Use this tab	To specify	See page
ViewPoint	ViewPoint application options, including custom call alert settings.	11-102
Sharing \ Call Monitor, Sharing \ Call Log, Sharing \ Contact, Sharing \ Message	If and how any of the user’s folders are shared with other users.	11-105

The User tab

You use the User tab to identify a user, assign an extension, create a password, and specify the user’s phone type and model.



● Slot:port: Slot 1 (Analog), Port 4

○ IP phone MAC address:

Telephone type: Analog

Access profile: Unrestricted

You can add a new user quickly via the User tab. When you add a new user, the only required fields are **Last name**, **Extension**, and **Password/Confirmation**. You can create a new user with with only this information provided, then edit the users at a later time to customize the user’s profile.

To add a new user via the User tab

1 In the User/Group Management applet, choose **File > New > User**, then click **User** in the left pane.

Identifying the user

2 **Required:** Enter the user's **First name** (up to 64 characters) and **Last name** (up to 30 characters).

3 Optionally, enter the user's **Title** (up to 30 characters) that you want to be displayed along with the user name in the User view.

You can use the **Title** field for various purposes, for example for the user's department. When a caller requests to be transferred to someone in Sales, the Operator can see all the users in the Sales department grouped together in ViewPoint's Transfer Call dialog. You can also use ViewPoint Groups to group users by department (see "About public and personal ViewPoint Groups" on page 12-2).

Assigning an extension

4 **Required:** Enter the user's **Extension**. A user's extension is the number callers dial to reach the user. Extensions must comply with the following restrictions:

- Must match the First Digit rules for length and digits allowed
- No longer than 10 digits
- Numeric characters only
- Must be unique

Note: Extension 8888 is reserved and cannot be assigned to an individual user. Extension 8888 is reserved for the "send message to all users" feature. If a user enters extension 8888 when sending a voice message from his or her phone, the message is automatically sent to all users who have a voice mailbox configured.

In addition, follow these recommendations when assigning extensions:

- Avoid extensions that begin with another extension or access code. For example, if one user is given extension 17 and another extension 177, users who dial extension 17 will experience a brief delay while Wave waits to see if another “7” is dialed.
- Avoid extensions that begin with the same number used for an auto attendant menu choice. Slow dialers may be unable to dial the extension at the auto attendant, because they will activate the menu choice instead. See “Creating a new auto attendant” on page 13-3.
- Avoid extensions that begin with frequently dialed area codes—if users forget to dial an access code, they may unexpectedly dial the extension instead. For example, if 1-617 is a commonly dialed prefix for your location, do not assign extension 161.

Creating a password

5 **Required:** Enter a numeric **Password** used to access the user's voicemail and account options, and to log on to ViewPoint. The user’s password can be changed either on this tab or in ViewPoint.

Retype the new password in the **Confirmation** field.

Note: Assigning secure passwords is one of the key means by which you can protect your business from unauthorized access, and lost money due to toll fraud. See Appendix Appendix A.

To set password requirements for the system such as minimum password length, click **Tools > System Settings** to use the “Recommended minimum password security settings” on page 4-14.

Specifying a phone type and model

6 Use the fields under **Associated device** to specify the user’s phone type and model:

- **Analog or digital phone user:** Select the appropriate slot and port for that phone from the **Slot:port** drop-down lists. (You can also assign a digital phone to a user automatically when you connect the phone as described in “Assigning a user from a digital phone” on page 11-18.)
- **SIP phone user:** Select **IP phone MAC address** and then enter the MAC address of the user’s IP phone.

- **Softphone user (ViewPoint Softphone or third-party softphone):** Due to a known issue that will be addressed in a future version, you must select **IP phone MAC address** even though this setting does not apply to softphone users. Enter any 12-digit string in the text box—for tracking or reference purposes, you can enter the MAC address of the user's primary PC that will be running the softphone.
- **For a user at a remote location or a cell phone user:** From the **Slot:port** drop-down lists, select **No slot selected** and **No port selected**.

7 Select the user's phone model from the **Telephone type** drop-down list.

- **To specify the ViewPoint Softphone as the user's primary phone**, select "ViewPoint Softphone".
- **To specify the ViewPoint Softphone as the user's secondary phone**, select the user's physical phone model.
- **To specify another softphone as the user's primary phone**, select "IP Third Party SIP Telephone".

8 Select an **Access profile** from the drop-down list. The access profile that you select specifies what type of outbound calls the user is permitted to make. "Unrestricted" enables the user to make all outbound calls.

The list of access profiles displayed here is set up in the Outbound Routing applet. See "Configuring specific access profiles" on page 9-14.

9 Click **OK** to save the new user with the current settings, or continue configuring the user via the other tabs of the User dialog.

Assigning a user from a digital phone

You can also assign a digital phone to a user automatically when you connect the phone.

To assign a user from a digital phone

1 Create the user as described in "The User tab" on page 11-15. Be sure to specify the following:

- Set **Slot:port** to **No slot selected** and **No port selected**.
- Select the digital phone model number of the phone to be assigned to this user from the **Telephone type** drop-down list.

2 Connect the phone to a digital phone port on the Wave Server.

3 If the phone was previously set up and plugged into a different port, the phone will display **Previous <Ext> Keep?**.

- If you are moving the phone but still want to keep it assigned to the same user, select **Yes**. Go to step 5.
- To assign the phone to a different user, select **No**.

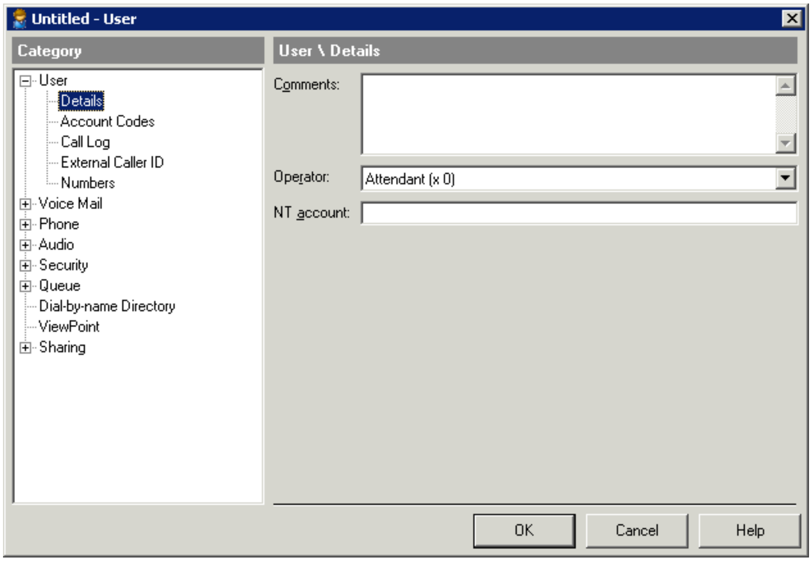
4 Press **BEGIN**. The phone displays a list of users who do not yet have a phone assigned, and whose **Telephone type** field matches the phone's. Scroll through the list and select the user to assign to the phone.

5 Press **Select** to choose the user to assign to the phone.

6 Press **Yes** to confirm the new phone assignment.

The User \ Details tab

You use the User \ Details tab to enter descriptive comments and other information about the user.



Untitled - User

Category

User \ Details

Comments:

Operator: Attendant (x 0)

NT account:

This section describes the following:

- Entering comments. See page 11-20.
- Setting up a personal operator. See page 11-20.
- Entering the user's Microsoft Windows NT account. See page 11-20.

Entering comments

On the User \ Details tab, use the **Comments** field to enter descriptive comments about the user as needed.

Setting up a personal operator

By default, Wave dials the Operator user's extension whenever a caller presses 0 while listening to a user's greeting or leaving a message.

To transfer calls to another user instead (for example, a departmental operator, personal assistant, or other auto attendant), select the user to whom you want to transfer calls from the **Operator** drop-down list on the User \ Details tab. For more information about operators, see "The Admin user" on page 11-3. A personal operator can be also be set in ViewPoint.

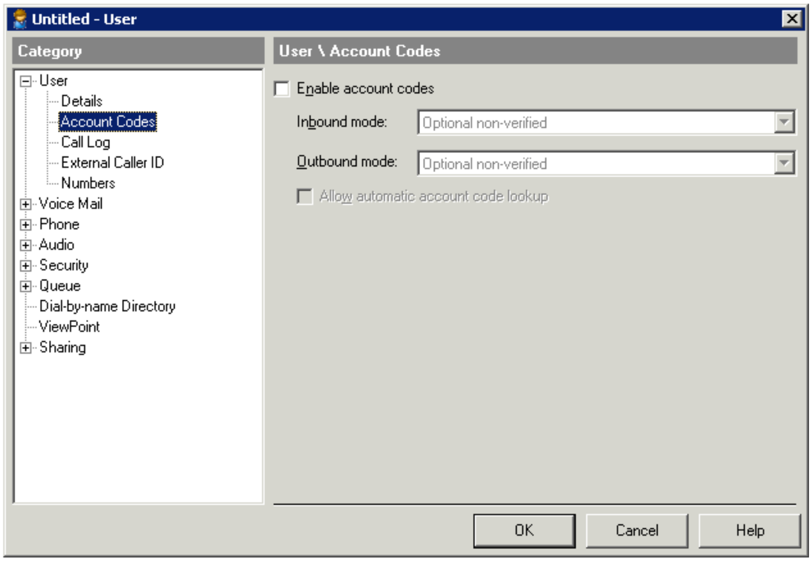
Entering the user's Microsoft Windows NT account

On the User \ Details tab, in the **NT account** field enter the user's Windows network account name, for example, MAIN\MAnatolia or WORKGROUP\John. This field is primarily for use by Add-ins and Client API developers.

The User \ Account Codes tab

Account codes are digits that users can enter to accompany each call that can then be used for billing or tracking purposes.

You use this tab to specify whether Wave will prompt this user to enter account codes.



Untitled - User

User \ Account Codes

□ Enable account codes

Inbound mode: Optional non-verified

Outbound mode: Optional non-verified

□ Allow automatic account code lookup

You set account code behavior separately for inbound and outbound calls. For outbound calls, you can handle account codes differently for long-distance calls vs. local calls.

You can also specify whether entered account codes are verified against a list of valid account codes that you create (as described in "Creating a valid account code list" on page 20-16). Note that if you select one of the "verified" options, Wave will reject invalid account codes until a valid one is entered.

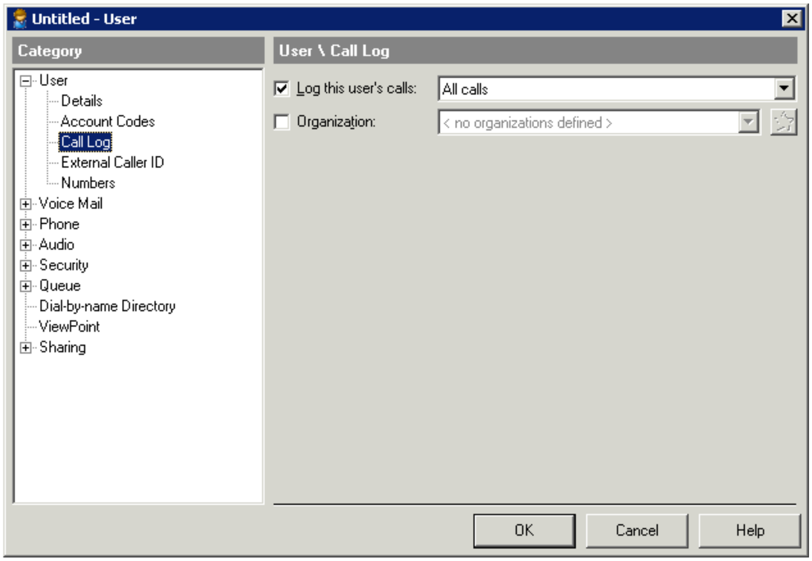
For more about how account codes are used in Wave, see "Using account codes" on page 20-10.

To configure the user’s account code settings

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the User \ Account Codes tab, select the **Enable account codes** checkbox to enable account code processing for this user.
3. For **Inbound mode**, select one of the following settings to apply to inbound calls placed to this user.
   - **Optional non-verified**. Do not prompt the user to enter account codes. If the user enters an account code, accept it without verification.
   - **Optional verified**. Do not prompt the user to enter account codes. If the user enters an account code, verify it.
4. For **Outbound mode**, select one of the following settings to apply to outbound calls placed by this user.
   - **Optional non-verified**. Do not prompt the user to enter account codes on outbound calls. If the user enters an account code, accept it without verification.
   - **Optional verified**. Do not prompt the user to enter account codes on outbound calls. If the user enters an account code, verify it.
   - **Forced non-verified - All calls**. Prompt the user to enter an account code on all outbound calls, if one has not already been entered. Accept the account code without verification.
   - **Force verified - All calls**. Prompt the user to enter account code on all outbound calls, if one has not already been entered, and verify it.
   - **Forced non-verified - Long distance calls only.** Prompt the user to enter an account code on all outbound long-distance calls, if one has not already been entered. Accept the account code without verification.
   - **Force verified - Long distance calls only.** Prompt the user to enter account code on all outbound long-distance calls, if one has not already been entered, and verify it.
5. Select the **Allow automatic account code lookup** checkbox to enable automatic association of account codes with contacts for this user. If checked, the user can enter an account code for each contact, and the system automatically applies the account code to all subsequent calls to and from the contact.

The User \ Call Log tab

The User \ Call Log tab lets you define how the user's calls appear in the Call Log in terms of which calls are logged, whether they are associated with an Organization, and what happens if the user logs onto another user's station. For more information, see "Using the Call Log view" on page 22-5.



☑ Log this user's calls: All calls

□ Organization: < no organizations defined >

This section describes the following:

- Determining which calls are logged. See page 11-23.
- Associating the user with an Organization. See page 11-24.

Determining which calls are logged

By default, all inbound and outbound calls made by the user appear in the Call Log. However, there are times when you might not want to log a user's calls due to space or readability reasons, for example if the user's station is connected to a fax server used for sending thousands of faxes daily.

To turn call logging on or off for the user

In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

- To turn off call logging for the user, on the User \ Call Log tab deselect the **Log this user's calls** checkbox.
- To specify which calls are logged for the user
  - Select the **Log this user's calls** checkbox.
  - Select **Only calls received**, **Only calls placed**, or **All calls** from the drop-down list.

Note the following:

- Users with call logging turned off cannot use ViewPoint's callback feature (**File > Return Last Call**) or the list of recently dialed calls on ViewPoint's File menu.
- If you have turned off internal call logging at the system level (see "Setting Call Log options" on page 22-9), the user's internal calls will not be logged, regardless of this setting.

Associating the user with an Organization

Organizations are a way to set up departments or multiple companies that share an office and a Wave Server. If you have created one or more Organizations, you can associate the user with the Organization to which he or she belongs. Calls that the user places or receives will be logged with that Organization showing in the Call Log's Organization column.

See "Using Organizations" on page 20-2.

To associate the user with an Organization

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 On the User \ Call Log tab, select the **Organization** checkbox, and select an **Organization** from the drop-down list.

If unchecked, the user's calls will appear in the Call Log with the Organization column blank.

The User \ External Caller ID tab

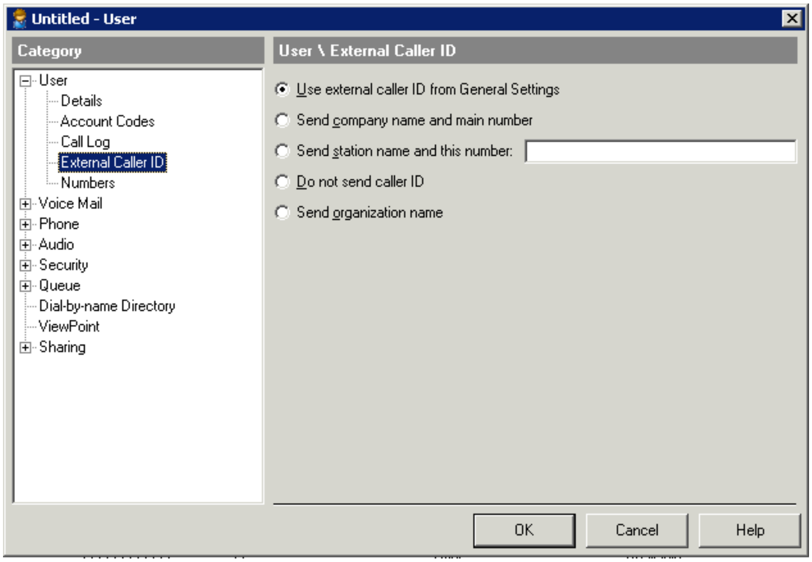
You can customize the Caller ID number and name that accompany outbound calls placed by the user. Note that the user can make his or her own selection in ViewPoint, but cannot specify a different custom number or name. If the user selects Custom, the Caller ID number and name are what is entered here.

By default all users send the External Caller ID format specified in the General Settings applet (see “Configuring system-wide Caller ID settings” on page 16-11). This procedure is only necessary if you want to override the system-wide Caller ID settings for a user.

To configure user-specific external Caller ID settings

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 Click the User \ External Caller ID tab.



Untitled - User

User \ External Caller ID

● Use external caller ID from General Settings
○ Send company name and main number
○ Send station name and this number:
○ Do not send caller ID
○ Send organization name

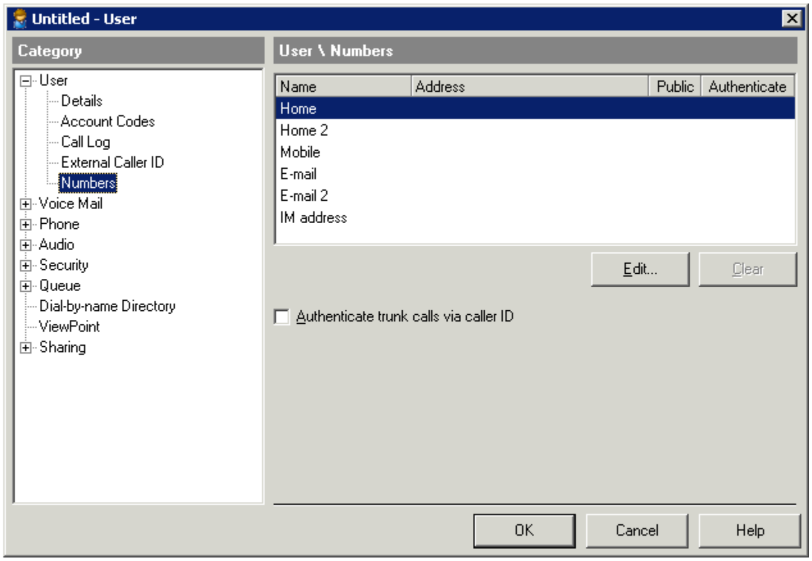
3 Select an External Caller ID setting:

- **Use External Caller ID from General Settings**. Sends the default settings configured in the General Settings applet.
- **Send Company Name and Main Number**. Sends the Company Name and Company Main Number as entered in the General Settings applet.
- **Send Station Name and this Number.** Sends the phone's station name Display Name as entered in the User Configuration (Templates) applet followed by the digits you enter here.

  Use this setting to provide the station name and number on outbound calls.
- **Do Not Send Caller ID.** Caller ID is not sent.
- **Send organization name**. Sends the name of the organization to which the user has been assigned via User dialog \ Call Log tab.

The User \ Numbers tab

You use the User \ Numbers tab to view and edit the numbers that appear in the user's "My Numbers" list in ViewPoint.



Name	Address	Public	Authenticate
Home			
Home 2			
Mobile			
E-mail			
E-mail 2			
IM address			

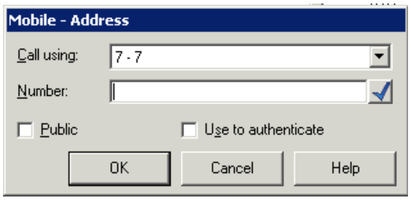
□ Authenticate trunk calls via caller ID

You also use this tab to enable automatic login for the user by authenticating one or more of the user’s numbers. When the user calls Wave from an authenticated number, he or she is automatically logged in without being prompted to enter an extension or password if automatic login is enabled for the called auto attendant. To enable automatic logon for an auto attendant, see “Creating a new auto attendant” on page 13-3.)

To enter or edit the user’s number

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 On the User \ Numbers tab, select the type of number you want to enter or modify, for example **Home** or **Mobile**, then click **Edit**. The Address dialog opens for the type of number that you selected.



Mobile - Address

Call using: 7 - 7

Number:

□ Public □ Use to authenticate

3 If the **Call Using** field is present, select the dialing service to use when placing calls to this number.

4 In the **Number**, **Address**, **Email**, or **IM address** field, enter the phone number, IP address, email address or instant messaging address.

5 Select the **Public** checkbox to make the number publicly available. Public numbers act as follows:

- Other users can quick-dial a public number (or make speed-dial shortcuts to them) by right-clicking the user’s name in their ViewPoint Extensions list.
- When a call comes into Wave from a public number, the user’s name appears in the **From** column in the ViewPoint Call Monitor, and can be used to identify the user.

  Note that in cases where the same number is defined in different places, Wave chooses the name to display by prioritizing as follows: (1) a user’s public number, (2) a public contact, (3) a private contact.
- Other programs can access the number, for example, a ViewPoint Add-in that automatically dials certain numbers.

If this checkbox is not selected, other programs cannot read or access the number.

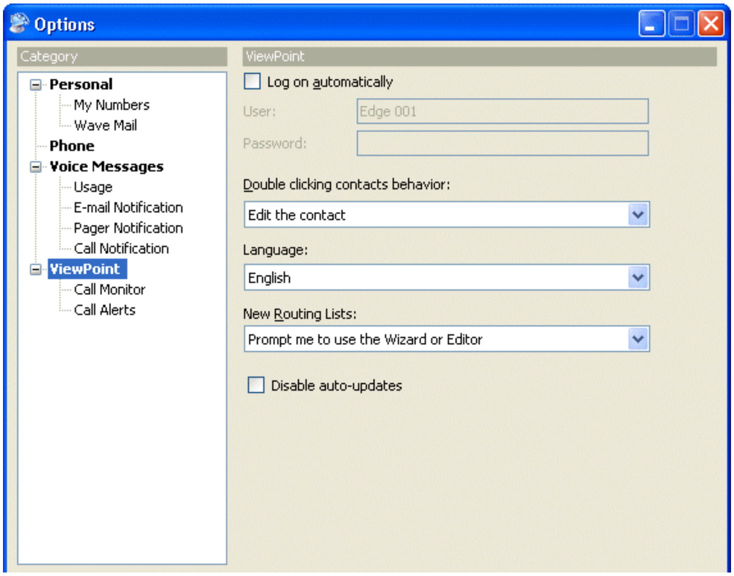
Note: You can also authenticate an existing number by selecting it on the User \ Numbers tab and selecting the **Authenticate trunk calls via caller ID** checkbox.

6 Select the **Use to authenticate** checkbox to enable automatic login for the selected number. If selected, whenever the user calls into Wave from this number via an auto attendant with automatic login enabled, he or she is automatically logged in without being prompted to enter an extension or password.

7 Click **OK** to return to the User dialog. To delete one of the user's numbers, select it, then click **Clear**.

The Voice Mail tab

You use this tab to configure various voice mailbox options for the user.


Options

Category
- Personal
  - My Numbers
  - Wave Mail
- Phone
- Voice Messages
  - Usage
  - E-mail Notification
  - Pager Notification
  - Call Notification
- ViewPoint
  - Call Monitor
  - Call Alerts

ViewPoint

□ Log on automatically

User: Edge 001

Password:

Double clicking contacts behavior: Edit the contact

Language: English

New Routing Lists: Prompt me to use the Wizard or Editor

□ Disable auto-updates

This section describes the following:

- Configuring the user’s voice mailbox. See page 11-29.
- Choosing the mailbox for call recordings. See page 11-29.
- Enabling voicemail greeting logon. See page 11-30.
- Synchronizing a user’s Wave voice messages and contacts with the user’s e-mail program. See page 11-30.

Configuring the user’s voice mailbox

On the User \ Voice Mail tab, in **Mailbox with __ minute max size**, enter the maximum size of the mailbox, in minutes. Mailboxes can be as large as 999,999 minutes (447 GB).

Choose the default setting of 20 minutes (9.2 MB of storage) for typical users. You may need to increase the default for users who record calls, because call recordings (including those that were e-mailed to the user) are stored in the user's mailbox.

Note: Voice messages take up disk space on the Wave Server computer. Once available disk space becomes scarce, system performance will suffer. To avoid this problem, archive your users’ voice messages and call recordings regularly. See “Archiving call recordings and voicemail” on page 22-24.

To create an extension without a voice mailbox—for example, a conference room or fax machine—click **No mailbox.**

Choosing the mailbox for call recordings

By default, call recordings that the user makes manually from ViewPoint’s Call Monitor are sent to the mailbox of the user who made them. To send personal recordings to another user’s mailbox instead, on the User \ Voice Mail tab select a name from the **Send personal call recordings to** drop-down list.

Note: This field applies only to call recordings manually made by the user. The destination for automatic call recordings made by the system is set separately. See “Recording all calls” on page 19-8.

Enabling voicemail greeting logon

By default, users can log on to their Wave accounts from a Wave station or auto attendant only. You can also allow this user log on by pressing 9 during the voicemail greeting. (In this case, the user is prompted only for password.) If you do not use auto attendants, you should enable this feature for all users, because it is the only way for them to access their accounts remotely. To enable the feature, select the **Allow voicemail log on during greeting by pressing 9** checkbox.

Note: Voicemail greeting logon can be slightly less secure than auto attendant logon, because the caller does not need to know the extension number. If you enable voicemail greeting logon, you should enforce secure passwords. See “Enforcing strong password security” on page 4-14.

Synchronizing a user’s Wave voice messages and contacts with the user’s e-mail program

WaveMail synchronizes a user’s voice messages and contacts between Wave and the user’s e-mail program. WaveMail allows the user to:

- Receive, listen to, and manage voice messages from either Wave or the user’s e-mail program.
- Share and maintain a single set of contacts between Wave and the user’s e-mail program.

See the following sections:

- WaveMail requirements. See page 11-31.
- How voice message synchronization works. See page 11-31.
- How contact synchronization works. See page 11-34.
- Configuring your e-mail provider for WaveMail. See page 11-35.
- Configuring a user’s WaveMail mailbox. See page 11-40.

WaveMail requirements

E-mail provider requirements

An e-mail provider is the external e-mail system that integrates with WaveMail for the purposes of voice message and contact synchronization.

WaveMail works with the following e-mail providers.

- Microsoft Exchange 2007, Service Pack 2 (SP2)
- Microsoft Exchange 2010

Important! WaveMail supports only internal (same network), non-hosted Exchange Servers. External, hosted Exchange Servers cannot be used.

A user can use an e-mail program supported by these providers to access shared voice messages and contacts, for example Microsoft Outlook.

License requirements

WaveMail is included with Wave. No additional licenses are required.

How voice message synchronization works

This section describes the following:

- How voice message folders are used. See page 11-32.
- How users can listen to and act on synchronized voice messages. See page 11-33.
- About potential conflicts between WaveMail and Exchange or Outlook rules. See page 11-33.

How voice message folders are used

After WaveMail is enabled and configured for a user, all of the user’s existing Wave voice messages (New, Saved, and Deleted) are sent to the user’s e-mail program and stored in the following folders:

Wave voice message status	E-mail program destination folder
New	Inbox
Saved	Wave Saved Messages
Deleted	Deleted Items

WaveMail continues to monitor activity in these two sets of folders.

- After the user’s voice messages are synchronized for the first time, all subsequent new Wave voice messages are automatically delivered to the user’s e-mail Inbox folder as well.
- If a user moves a message between the folders on the Wave side, WaveMail moves it accordingly on the Exchange side. Similarly, if a user moves a message between the folders on the Exchange side, WaveMail moves it accordingly on the Wave side.
- WaveMail maintains synchronization of the Heard/Unheard (Read/UnRead), Urgent/Normal, and Private/Normal message states in the folders on both sides.
- If a user moves a message to any other folder on the Exchange side, WaveMail permanently deletes the message on the Wave side.
- If a user renames the Wave Saved Messages folder, WaveMail continue to use it with the new name.
- If a user deletes the Wave Saved Messages folder on the Exchange side, WaveMail will re-create it automatically the next time it needs it to synchronize a message residing in the Saved folder on the Wave side.

How users can listen to and act on synchronized voice messages

With WaveMail, the user can listen to and manage voice messages in any of the following ways:

- Via the phone, using the phone commands. See the *Wave Phone User Guide* for details.

  Note: Standard phone behavior in Wave is that only Unheard messages in the Inbox are included in the New message count on the LCD of the user's phone. Also, the Message Waiting Indicator on the phone is lit only if the Inbox contains at least one Unheard message. This behavior is the same whether the user changes the number of Unheard messages in the Inbox on the Wave side or the Exchange side (for example, by listening to or reading a message, deleting an Unheard message, moving it to another folder, and so forth.)

- Via ViewPoint. See Chapter 7 in the *Wave ViewPoint User Guide*.
- Via the user's e-mail program. See its documentation for details.

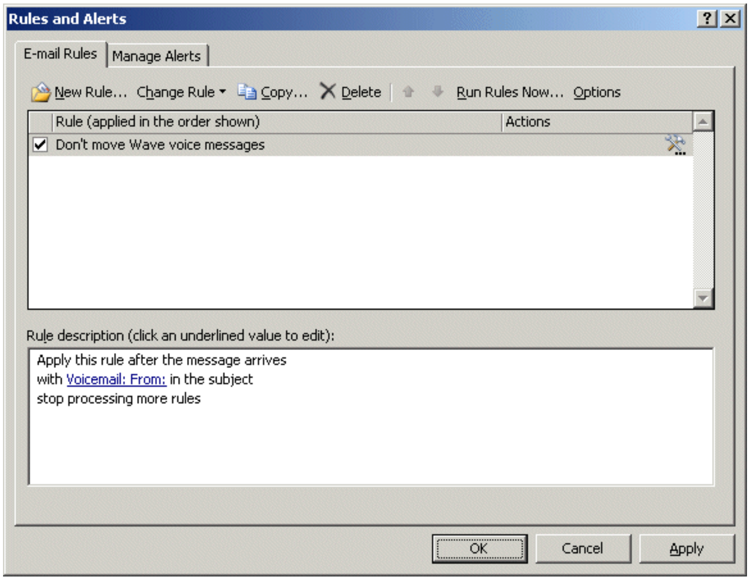
About potential conflicts between WaveMail and Exchange or Outlook rules

If a user has Exchange or Outlook rules for processing messages, it is possible that one or more rules may be executed on a message that interfere with the expected synchronization between WaveMail and Exchange. For example, a rule might move a message to another folder, causing a voice message to be deleted before the user has a chance to listen to it.

To avoid conflicts between WaveMail and Exchange or Outlook rules

1. Define a new rule and make it the first rule to be executed before any other rules.
2. Configure that rule to identify incoming voice messages delivered to the user's Exchange Inbox by WaveMail. For example, the rule could search for "Voicemail: From" in the message subject, or use other identification logic that applies to a particular user.

3 Add an action that if the rule identifies an incoming voice message delivered by WaveMail, stop processing all other rules. For example, an Outlook rule might look like this:



☑ Don't move Wave voice messages

Rule description (click an underlined value to edit):

Apply this rule after the message arrives
with Voicemail: From: in the subject
stop processing more rules

How contact synchronization works

After WaveMail is enabled and configured for a user, all of the user's existing Wave contacts and e-mail contacts are compared. Duplicate contacts are processed so that Wave and the e-mail program end up with a single set of matching contacts. (Duplicates are determined primarily by a name match, but address matching—phone numbers, e-mail addresses, and so forth—are also used to determine a match.) When you configure WaveMail for the user, you specify whether you want to use the information in the Wave contact or the e-mail contact to take precedence in case of a conflict.

With WaveMail, the user can manage contacts in ViewPoint or via his or her e-mail program. After the user's contacts are synchronized for the first time, WaveMail monitors both contact lists for subsequent additions, changes, and deletions and updates Wave and the e-mail program as necessary to keep both contact lists synchronized.

Configuring your e-mail provider for WaveMail

Before you can configure WaveMail mailboxes for an individual users, you must perform the following tasks to configure your e-mail provider. Note that in this version, the supported e-mail providers are Microsoft Exchange 2007 Service Pack 2 (SP2) and Microsoft Exchange 2010.

- **Create the WaveMail user impersonation account** in Windows.
- **Add the permission to impersonate to the WaveMail user** via the Exchange Management Shell to give impersonation privileges to WaveMail.
- **Create an Exchange mailbox for the WaveMail user** via the Exchange Management Console.
- **Configure your e-mail provider as a WaveMail provider** via the General Settings applet in the Global Administrator Management Console.

To configure Microsoft Exchange for WaveMail

1. Click **Start > Active Directory Users and Computers**.
2. Create the WaveMail impersonation user account. The password for this account should be set to not expire.
3. Click **Start > Exchange Management Shell**.
4. Depending on your version of Microsoft Exchange, do one of the following to add the permission to impersonate to the WaveMail user that you created in step 2.

   Note: The name that you specify in the `-User` parameter below must exactly match the user name that you entered for the WaveMail user account in step 2.

   Important! If you do not specify the following information accurately, Microsoft Exchange will not be configured correctly and WaveMail synchronization will not work. Be absolutely certain that you type or copy/paste the following EXACTLY as specified—do not introduce extra quotation marks or new lines. Also, be sure to use the information for your version of Microsoft Exchange.

   - **Microsoft Exchange 2007 SP2:**

     Enter the following and then click **Enter**:

     ```
     “Get-ExchangeServer | where {$_.IsClientAccessServer -eq
     $TRUE} | ForEach-Object {Add-ADPermission -Identity
     $_.distinguishedname -User (Get-User -Identity WaveMail |
     select-object).identity -extendedRight
     ms-Exch-EPI-Impersonation}”
     ```

Enter the following and then click **Enter**:

```
“Get-MailboxDatabase | ForEach-Object {Add-ADPermission
-Identity $_.DistinguishedName -User WaveMail
-ExtendedRights ms-Exch-EPI-May-Impersonate}”
```

- **Microsoft Exchange 2010:**

  Enter the following and then click **Enter**:

  ```
  “new-ManagementRoleAssignment -Name:_suImpersonateRoleAsg
  -Role:ApplicationImpersonation
  -User:’accountname@sitedomain’”
  ```

5. Click **Start > Exchange Management Console**.
6. Expand **Recipient Configuration > Mailbox**, and then choose **Actions > New Mailbox**. Follow the onscreen instructions to create a new User Mailbox for the WaveMail impersonation user account that you created in step 2.

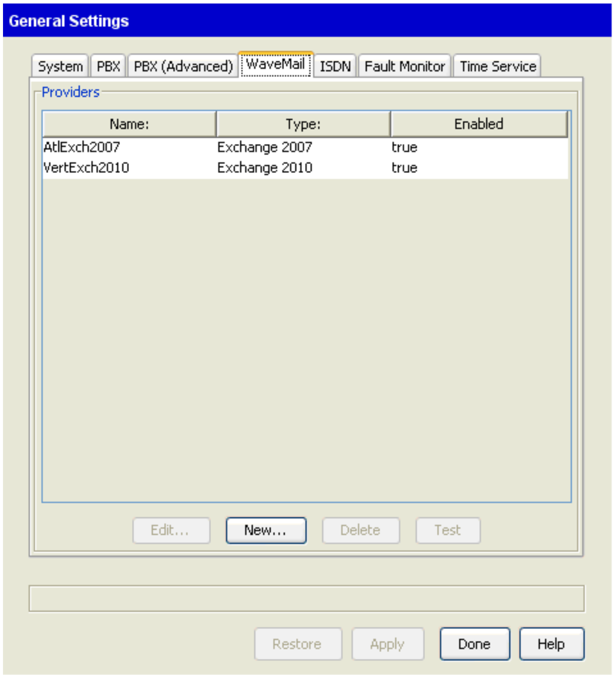
To configure your e-mail provider as a WaveMail provider

1. If necessary, click the Administration tab of the Management Console.

Click

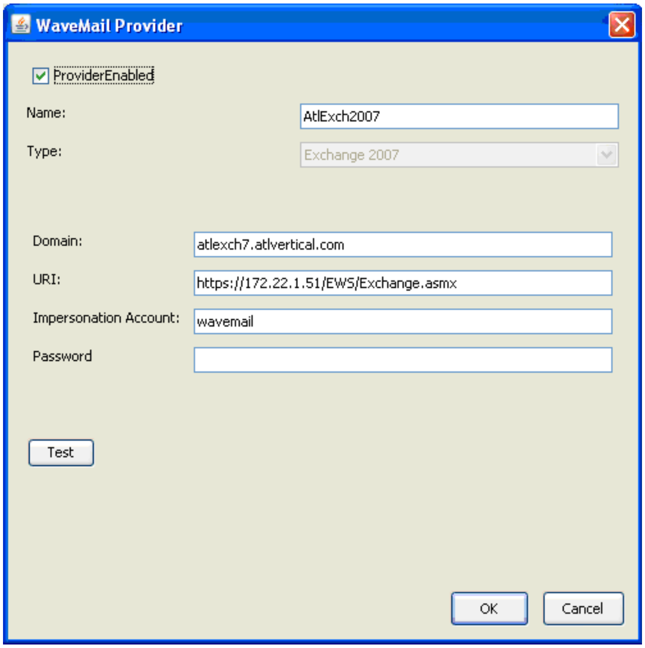
2. Click the General Settings icon, located in the General Administration section.

3 Select the WaveMail tab. Any e-mail providers that have already been configured are listed.



Name:	Type:	Enabled
AtlExch2007	Exchange 2007	true
VertExch2010	Exchange 2010	true

4 Click **New** to add a new e-mail provider. The WaveMail Provider dialog opens:



WaveMail Provider

☑ ProviderEnabled

Name: AtlExch2007

Type: Exchange 2007

Domain: atlexch7.atlvertical.com

URI: https://172.22.1.51/EWS/Exchange.asmx

Impersonation Account: wavemail

Password

5 Enter the **Name** of this e-mail provider, for example, the name of the Exchange Server.

6 Select the version of your e-mail provider from the **Type** drop-down list.

Important! Be sure to select the entry for your version of Microsoft Exchange (2007 or 2010)—selecting the wrong version will prevent WaveMail from operating correctly. Note that you cannot change an e-mail provider’s type after you create it.

7 Enter the following information:

- **Domain**. Domain for user accounts on the Exchange Server, for example "mycompany.com". The format of the domain name that you enter here depends on the version of Microsoft Exchange that you are using as your e-mail provider:

  Note: There are many different ways to configure domains in Exchange, and the examples provided below may not apply in your environment. If you are not sure how to enter your domain name here, contact Vertical Technical Support.

  - **Exchange 2007 SP2:** Typically, you enter the *external* domain name, for example "abccompanies.com".
  - **Exchange 2010:** Typically, you enter the *internal* domain name, for example "abcmanufacturing.local".
- **URI**. Uniform Resource Indicator for WaveMail to use to connect to the Exchange Server, for example:

  https://mail.mycompany.com/EWS/Exchange.asmx
- **Impersonation Account**. User name for the Exchange impersonation user account used by WaveMail to synchronize with all other Exchange accounts on the Exchange Server. The user name and password that you enter here must exactly match what you specified when you created the impersonation user account in "Configuring your e-mail provider for WaveMail" on page 11-35.
- **Impersonation Password**. Password for the Exchange impersonation account used by WaveMail.

  Note: This password can be up to 128 characters long. All characters except "^" are allowed.

8 Select the **Provider Enabled** checkbox to enable WaveMail synchronization on this e-mail provider. One or more e-mail providers can be enabled at the same time. If this checkbox is not selected, synchronization on any WaveMail mailboxes defined for this provider does not occur.

9 Click **Test** to verify that WaveMail can successfully communicate with the Exchange Server as configured with the current settings. If the test fails, WaveMail mailboxes on that e-mail provider will not be synchronized until the problem is resolved.

Possible causes for failure include:

- **Incorrect Exchange version**. Be sure to select your version of Exchange (see step 6).
- **Invalid domain**. The domain you specify must exactly match what is in Exchange (see step 7).
- **Invalid URI**. Use the “Exchange.asmx” form—do not substitute variants like “Services.wsdl” (see step 7).
- **Incorrect impersonation account name**. Make sure that the impersonation account name exactly matches what is in Exchange (see step 7). Also, verify that the `–User` parameter exactly matches what is in Exchange when you grant impersonation rights to the WaveMail user account via the Exchange Management Shell (see step 4).
- **Incorrect impersonation password**. Make sure that the impersonation account password exactly matches what is in Exchange. See step 7.

10 When the new e-mail provider configuration is working correctly, click **OK**.

After you complete these tasks, go to the next section.

Configuring a user’s WaveMail mailbox

Before a user can begin synchronizing voice messages and contacts between Wave and his or her e-mail program, you must perform the following steps:

- Assign the user the appropriate Wave permission, **Synchronize voice mail and contacts**. You can assign this permission to the user, or add the user to a role that has this permission. See “The Security \ Permissions tab” on page 11-96 for details.
- Enable WaveMail for the user and configure the user’s WaveMail mailbox. A WaveMail mailbox is used to synchronize a user’s extension with your e-mail provider.

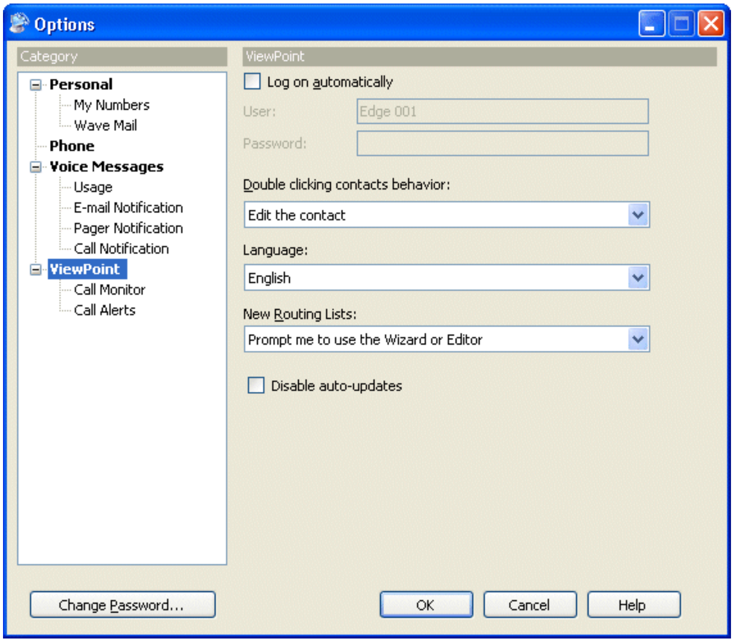
  You can perform these steps via the Voice Mail tab (described below), or you or the user can perform the same steps via the ViewPoint Options dialog (see Chapter 7 in the *Wave ViewPoint User Guide*).

Note: In ViewPoint, the WaveMail configuration fields will be disabled until you assign the Wave permission **Synchronize voice mail and contacts** to the user or user’s role.

To enable WaveMail and configure a user’s WaveMail mailbox

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 On the Voice Mail tab, enter the following information:



□ Log on automatically

User: Edge 001

Password:

Double clicking contacts behavior: Edit the contact

Language: English

New Routing Lists: Prompt me to use the Wizard or Editor

□ Disable auto-updates

3 Enter the following information. (You specified these values when you configured the user’s e-mail provider via the General Settings applet.)

- **Server**. Select the name of the user’s Exchange Server from the drop-down list.
- **Account name**. Enter the user name (for example “Scott Amaral”) or login name (“samaral”) of this user’s e-mail account—the account with which you want WaveMail to synchronize this user’s Wave voicemail and contacts.
- **Password**. Enter the password of the user’s e-mail account.

4 Select the **Synchronize voice mail and contacts** checkbox to enable synchronization for this user.

5 Select one of the following from the **In case of conflict keep my ___ settings** drop-down list. This setting determines which contact takes precedence if similar contacts exist in Wave and your e-mail program.

- **Wave**. The Wave contact information will be propagated to your e-mail program.
- **E-mail**. The e-mail contact information will be propagated to Wave.

The Voice Mail \ E-mail, Pager, and Call Notification tabs

You can have Wave notify a user by e-mail, page, or phone call whenever he or she receives a new voice message. This powerful feature enables users to keep abreast of their Wave voicemail no matter where they are. Notification messages include important details about the call, and give users quick access to hearing the message and responding to it. You have notifications sent for all voice messages or for Urgent messages only. You can also have notifications sent only at certain days or times. Notifications are sent only for new voice messages, not new call recordings that arrive in a user’s Inbox.

Users can also configure notifications in ViewPoint.

Note: Paging and call notification will not work with access codes that route over PRI trunks unless you make configuration changes. See “Enabling trunks for external pager and call notifications” on page 5-42 for details.

This section describes the following:

- Notification information. See page 11-43.
- Determining which voice messages send notification. See page 11-44.
- Setting e-mail notification. See page 11-44.
- Setting pager notification. See page 11-46.
- Setting call notification. See page 11-48.
- Scheduling notifications. See page 11-49.
- Defining a schedule for notifications. See page 11-50.
- Setting up custom hours. See page 11-52.

Notification information

The following information is attached to notifications of each type, making them a powerful tool for voicemail management, even at a remote location.

E-mail notifications can contain:

- Caller’s name
- Phone number at which the call originated
- Wave extension at which the message was left
- Voice message length
- Notes associated with the message
- Voice message as a WAV file attachment

Pager notifications can optionally contain:

- Caller ID for message
- Wave extension that was dialed
- Voice message length

Call notifications contain:

- Voice title of the user who received the message
- Voice title or recorded name of the person who left the message, if available
- Identification of urgent messages
- Length of the voice message
- Ability to press **#** right from the call and hear the message, then press **43** to call them back.

Note: You can use call notifications to log onto your account from a remote location and have Wave pay for the call rather than your remote phone. See the *Wave ViewPoint User Guide*.

Determining which voice messages send notification

For each notification type—e-mail, pager, and call—you can define how often notifications are sent, using the following drop-down list options:

- **Do not send notifications**. The user does not receive notification of new voice messages.
- **Send notification for all messages**. The user receives a notification whenever new voice messages arrive.
- **Send for Urgent messages only**. The user receives a notification whenever voice messages marked Urgent arrive.

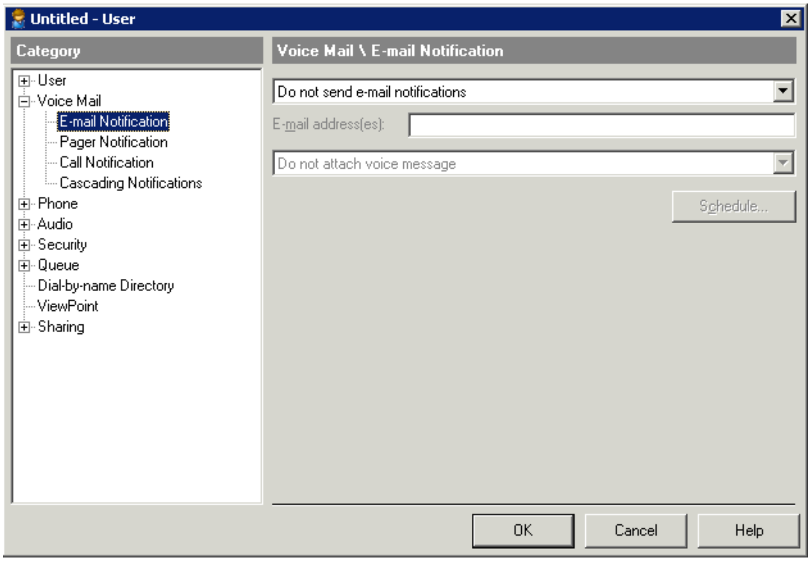
Setting e-mail notification

Before setting up e-mail notification for a user, make sure e-mail notification is configured properly on the Wave Server, as described in “Setting up e-mail notification” on page 4-12.

To set up e-mail notification

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 Click the Voice Mail \ E-mail Notification tab.


Untitled - User

Category: User; Voice Mail (E-mail Notification, Pager Notification, Call Notification, Cascading Notifications); Phone; Audio; Security; Queue; Dial-by-name Directory; ViewPoint; Sharing

Voice Mail \ E-mail Notification

Do not send e-mail notifications

E-mail address(es):

Do not attach voice message

3 Select whether e-mail notifications occur, and if so, how often. (See “Determining which voice messages send notification” on page 11-44.)

4 In the **E-mail address(es)** field, enter the e-mail address to which notifications are sent. Separate multiple addresses by semicolons (;).

Note: If using SMTP, valid e-mail addresses must be in the format of `user@company.com`. If using MAPI, e-mail addresses must be resolvable via the Microsoft Outlook address book.

5 In the next drop-down list, choose whether the voice message is attached to the e-mail as a WAV file, by selecting one of the following:

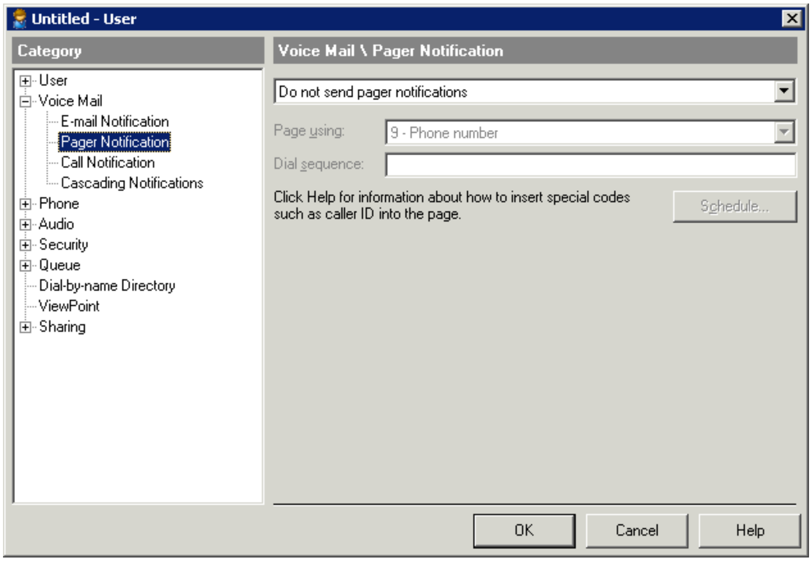
- **Do not attach voice message**. The voice message is not attached to the e-mail.
- **Attach voice message**. Messages are attached to the e-mail and also appear in the user’s Wave Inbox marked as unheard.
- **Attach voice message and mark as already heard**. Messages are attached to the e-mail and appear in the user’s Inbox marked as already heard.
- **Attach voice message and delete from Inbox**. Messages are attached to the e-mail only, and do not appear in the user’s Wave Inbox.

Setting pager notification

To set up pager notification

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 Select the Voice Mail \ Pager Notification tab.



Untitled - User

Category

- User
- Voice Mail
  - E-mail Notification
  - Pager Notification
  - Call Notification
  - Cascading Notifications
- Phone
- Audio
- Security
- Queue
- Dial-by-name Directory
- ViewPoint
- Sharing

Voice Mail \ Pager Notification

Do not send pager notifications

Page using: 9 - Phone number

Dial sequence:

Click Help for information about how to insert special codes such as caller ID into the page.

3 Select whether pager notifications occur, and if so, how often. (See “Determining which voice messages send notification” on page 11-44.)

4 In the **Page using** field, select the dialing service that you want Wave to use to dial the user’s pager.

5 In the **Dial Sequence** field, enter the dial string for the pager, including the phone number of the paging service and the pager's PIN if required. The dial string can contain any touch tone digit (0-9, *, #). You can also enter a comma to indicate a 2-second pause in the dial sequence.

You can also use the following special characters to add information to the page:

- I or i sends the Caller ID number (for an external call) or Wave extension (for an internal call).
- E or e sends the Wave extension that the caller dialed.
- L or l sends the length of the voice message in seconds.

For example, the dial sequence `18007771000,,,1245983#E` causes Wave to dial the paging service, pause for 6 seconds, enter the pager’s PIN (1245983) followed by # to indicate end-of-PIN, enter your extension (where the voice message was left), and then hang up. In this example, your pager displays only the extension number.

If users receive only the last portion of the pager data specified, there are not enough pauses between the pager number and the information. If this problem occurs, add more commas (each of which represents a 2-second pause.)

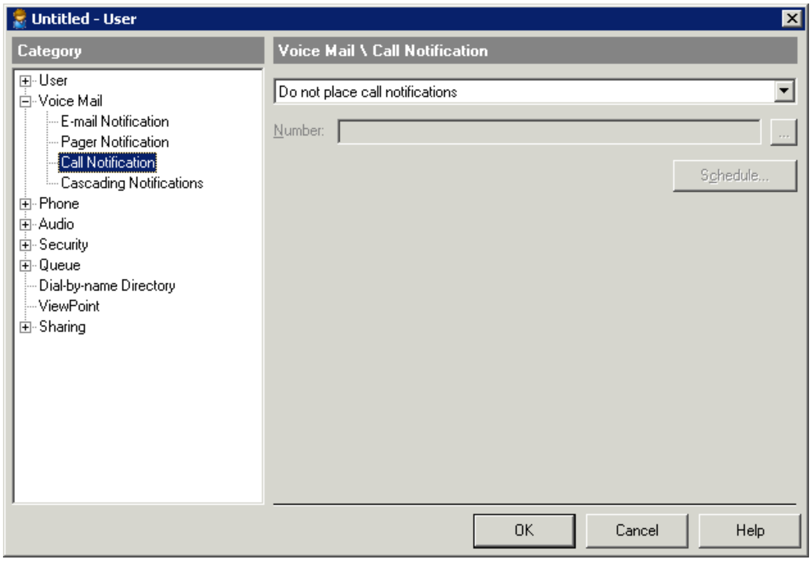
Note: Do not enter multiple stars (*) in a row in the pager string. Use only one star to send a dash. Multiple consecutive stars can terminate the page message.

Setting call notification

To set up call notification

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

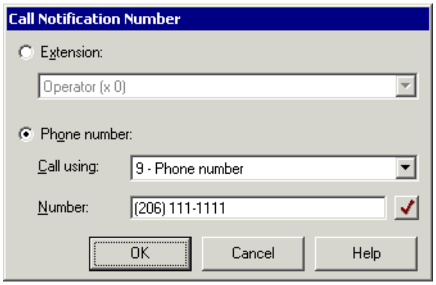
2 Select the Voice Mail \ Call Notification tab.



Do not place call notifications

3 Select whether call notifications occur, and if so, how often. (See “Determining which voice messages send notification” on page 11-44.)

4 Click ... in the **Number** field to open the Call Notification Number dialog.



○ Extension:

Operator (x 0)

● Phone number:

Call using: 9 - Phone number

Number: (206) 111-1111 ✓

5 Choose one of the following options:
   - Click **Extension** and select an extension from the drop-down list.
   - For an external number, use the **Call Using** drop-down list to select the access code and dialing service to use when placing notification calls. Then enter the number to dial in **Number**, exactly as it should be dialed.

6 Click **OK**.

Scheduling notifications

If you do not want to receive notifications 24 hours a day, 7 days a week, you can schedule notifications to occur at specific times only. For example, you can have Wave send notifications only during business hours or after business hours on work days. You can also set up custom hours. You can create different schedules for e-mail, pager, and call notification. Notifications can also be scheduled in ViewPoint.

Note the following:

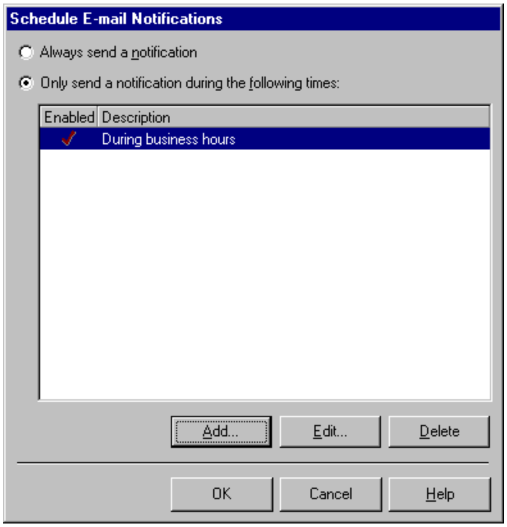
- When you turn notification on for a user, by default Wave sends notifications 24 hours a day, 7 days a week. If this is what you want to do, you do not need to schedule notifications.
- Notifications are never queued for later delivery. When you use a schedule, voice messages that arrive during an unscheduled time do not produce notifications at all.

A schedule contains individual schedule entries. For example, if you want a user to be notified of new voice messages during business hours and all day on holidays, you would add a schedule entry for “during business hours” and another schedule entry for “on holidays.” You (or users) can define custom schedule entries for even greater precision.

You can enable or disable each schedule entry as needed. For example, if you do not want a user to be paged during a specific upcoming holiday, disable the schedule entry for “on holidays.” You can enable it after the holiday has passed.

Defining a schedule for notifications

After setting the options in the e-mail, pager, or call section on the Notifications tab, click **Schedule** in the appropriate section to define a schedule for notification. The Schedule (E-mail/Pager/Call) Notifications dialog opens. The **Schedule** button is unavailable until you have created notification settings on the Notifications tab.



Schedule E-mail Notifications

○ Always send a notification

● Only send a notification during the following times:

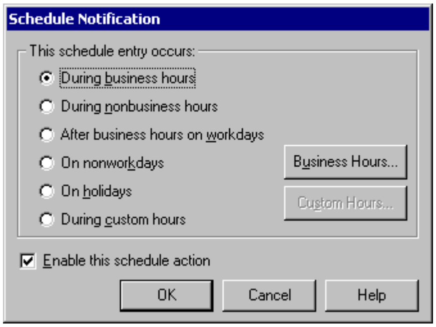
Enabled	Description
✓	During business hours

The Schedule Notifications dialog lists the schedules that have been defined so far, if any. Click one of the following:

- **Always send a notification**. The schedule entries in the list (if any have been created) are ignored, and the user receives notification of new voice messages at all times.
- **Only send a notification during the following times**. The user receives notification only during the times specified in the schedule entries that appear in the list with a check mark in the Enabled column.

To add a schedule entry

1 To add a schedule entry, click **Add**. The Schedule Notification dialog opens.



Schedule Notification

This schedule entry occurs:

● During business hours
○ During nonbusiness hours
○ After business hours on workdays
○ On nonworkdays
○ On holidays
○ During custom hours

☑ Enable this schedule action

2 To view or change the business and holiday hours used for scheduling, or to create other sets of business hours, click **Business Hours**. See “Setting business hours” on page 4-9.

3 Under **This schedule entry occurs**, choose one or more of the following time periods during which you want to notify the user of new voice messages. For purposes of illustration, each of the time periods in the following list show in parentheses what would be the result of selecting that time period in a company whose business hours are Monday through Friday, from 9:00 a.m. to 5:00 p.m.

- **During business hours**. Notifications are sent during business hours, Monday through Friday, from 9:00 a.m. to 5:00 p.m.
- **During nonbusiness hours**. Notifications are sent at all times other than business hours, including early mornings, evenings, weekends, and holidays. Notifications are sent Monday through Friday, 5:01 p.m. to 8:59 a.m., and on Saturdays, Sundays, and holidays.
- **After business hours on workdays**. Notifications are sent Monday through Friday, 5:01 p.m. to 8:59 a.m.
- **On nonworkdays**. Notifications are sent on Saturdays and Sundays.
- **On holidays**. Notifications are sent on holidays. See “Setting business hours” on page 4-9.
- **During custom hours**. Notifications are sent during specific days and hours independent of the business and holiday hours already defined. See Setting up custom hours“Setting up custom hours” on page 11-52.

4 Be sure to check **Enable this schedule action**, and then click **OK**. Now the schedule in the Schedule Notifications dialog includes the schedule entry you just created. Add more schedule entries as needed, and then click **OK** when you are finished.

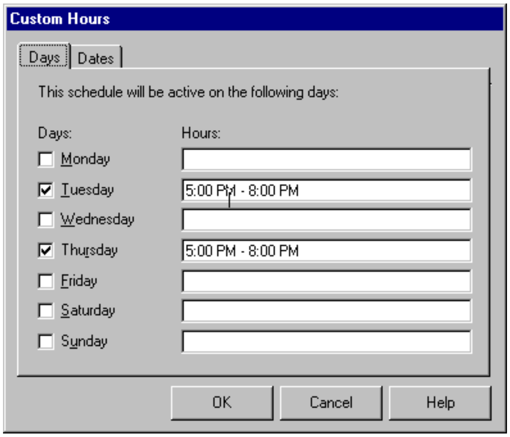
Setting up custom hours

You can define custom hours that are not related to your office’s business hours and holidays and use them to schedule notifications, auto attendant actions, and routing list actions. Custom hours are specific to the user, auto attendant, or routing list for which you create them. That is, the custom hours you set up for a user do not apply automatically to other users. Custom hours for a user can also be set up in ViewPoint.

When setting custom hours, you can enter dates and times in most formats—they are converted to a standard format based on your Windows regional settings.

To set up custom hours

1 Click **Custom Hours** in either the Schedule Notification dialog (for users) or the Schedule Action dialog (for auto attendants). The Custom Hours dialog opens.



Custom Hours

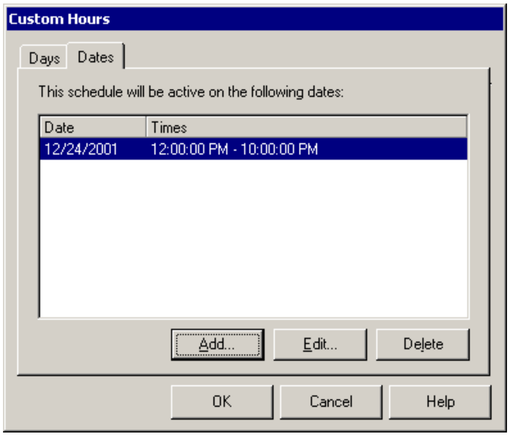
This schedule will be active on the following days:

Days:	Hours:
□ Monday	
☑ Tuesday	5:00 PM - 8:00 PM
□ Wednesday	
☑ Thursday	5:00 PM - 8:00 PM
□ Friday	
□ Saturday	
□ Sunday	

2 On the Days tab, check each day of the week for which you want the custom schedule to be active. If you leave the **Hours** field blank for a selected day, the entire day is included in the custom schedule. To include only part of a day, enter starting and ending hours.

Note: You can enter multiple time ranges separated by commas, for example, “9:00 AM - 12:00 PM, 3:00 PM - 6:00 PM.”

3 On the Dates tab, click **Add** if you want to apply the custom schedule to a specific date.

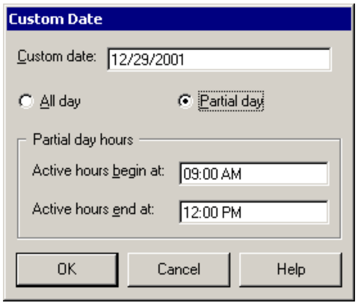


Custom Hours

This schedule will be active on the following dates:

Date	Times
12/24/2001	12:00:00 PM - 10:00:00 PM

4 In the Custom Date dialog that opens, enter the **Custom date**, and then click **All day** or **Partial day**. For a partial day, enter starting and ending times.



Custom Date

Custom date: 12/29/2001

○ All day ● Partial day

Partial day hours

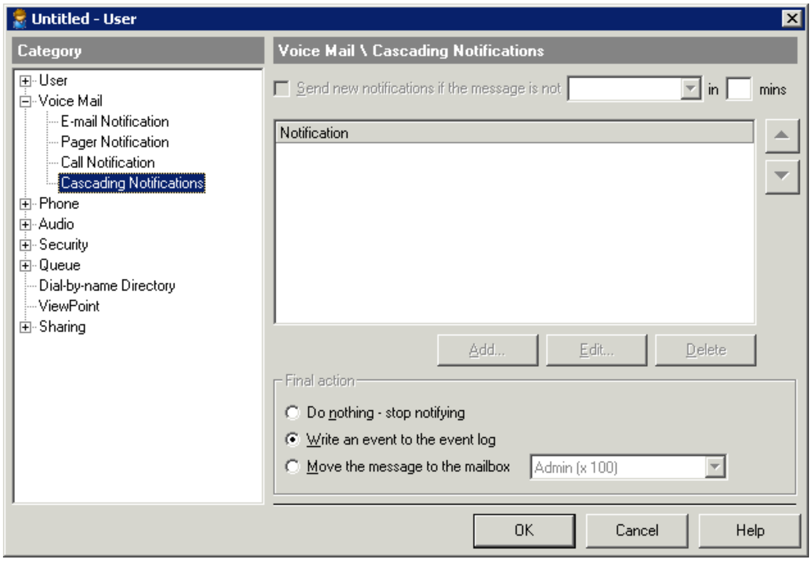
Active hours begin at: 09:00 AM

Active hours end at: 12:00 PM

5 Click **OK** to add the custom date to the list on the Dates tab of the Custom Hours dialog.

The Voice Mail \ Cascading Notifications tab

You use the Cascading Notifications tab to configure repeated (“cascading”) notifications if this user receives a new voice message and does not listen to or act on it within the period of time that you specify. IT staff or medical personnel in particular may need to rely on cascading notifications when it is critical that voice messages are listened to and handled within a specific period of time.



□ Send new notifications if the message is not [ ] in [ ] mins

Final action

○ Do nothing - stop notifying

● Write an event to the event log

○ Move the message to the mailbox Admin (x 100)

Cascading notifications supplement the standard voice mail notification feature, which sends a single notification for each type selected (e-mail, pager, or call notification).

Note: In order to configure cascading notifications for a user, the user must have at least one type of voice mail notification (e-mail, pager, or call) set, and the user must have a voice mailbox. If these requirements are not met, the options on this tab are disabled.

To set up cascading notifications for the user

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

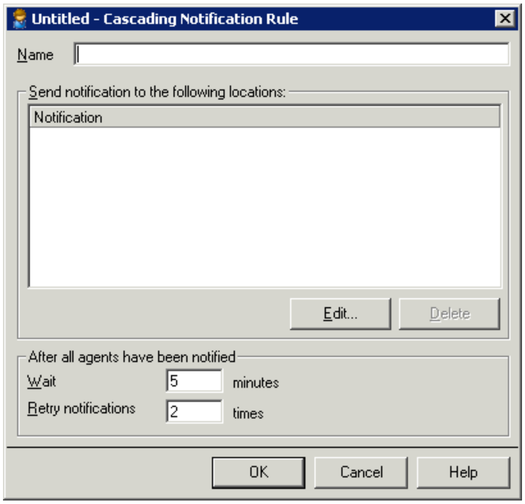
2 Click the Cascading Notifications tab. (The options on this tab are disabled if you have not set at least one type of voice mail notification for the user.)

3 Select the **Send new notifications** checkbox.

4 Complete the statement as follows:

- **if the message is not** ___. Select one of the following actions from the drop-down list:
  - **marked as heard**. Cascading notifications will be sent if the user does not listen to the new voice message.
  - **saved or deleted**. Cascading notifications will be sent if the user does not act on the new voice message by saving or deleting it.
- **in** ___ **mins**. Enter the number of minutes to wait for the action to occur.

5 Click **Add** to create a new cascading notification, or **Edit** to modify the selected notification. The Cascading Notification Rule dialog opens:


Untitled - Cascading Notification Rule
Name
Send notification to the following locations:
Notification
Edit...
Delete
After all agents have been notified
OK
Cancel
Help

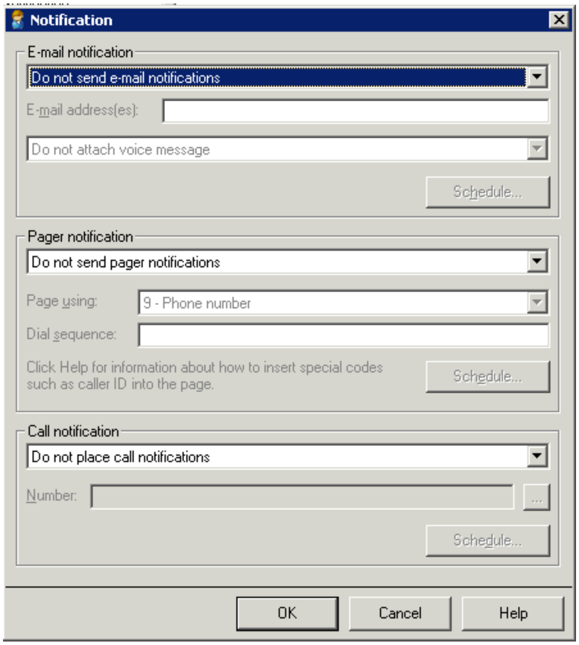
Wait 5 minutes

Retry notifications 2 times

6 Enter the following information:

- **Name**. Name of this set of cascading notifications.
- **Send notification to the following locations**. Lists each individual notification type and target that has been defined so far in this set of cascading notifications.

7 Click **Edit** to identify the specific e-mail, pager and call notification settings that make up this set of cascading notifications. The Notification dialog opens:



Notification

E-mail notification

Do not send e-mail notifications

E-mail address(es):

Do not attach voice message

Pager notification

Do not send pager notifications

Page using: 9 - Phone number

Dial sequence:

Click Help for information about how to insert special codes such as caller ID into the page.

Call notification

Do not place call notifications

Number:

For an explanation of how these fields work, see the following sections:

- “Setting e-mail notification” on page 11-44
- “Setting pager notification” on page 11-46
- “Setting call notification” on page 11-48
- “Scheduling notifications” on page 11-49

8 Click **OK** to return to the Cascading Notification Rule dialog.

9 In the **After all agents have been notified** section, define what happens if all of the individual notifications listed here have been sent and the voice message has still not been listened to or acted upon.

- **Wait ___ minutes**. Enter the number of minutes to wait before:
  - Retrying the individual notifications listed above (specify the number of times to repeat below).
  - Trying the next notification (if any) listed in the Cascading Notifications tab.
  - Performing the final action specified in the in the Cascading Notifications tab (see below for instructions).
- **Retry notifications ___ times**. Enter the number of times to repeat the individual notifications listed above before trying the next notification (if any) or performing the final action. Enter 0 if you want to make one attempt of the individual notifications listed above with no retries before trying the next notification or performing the final action.

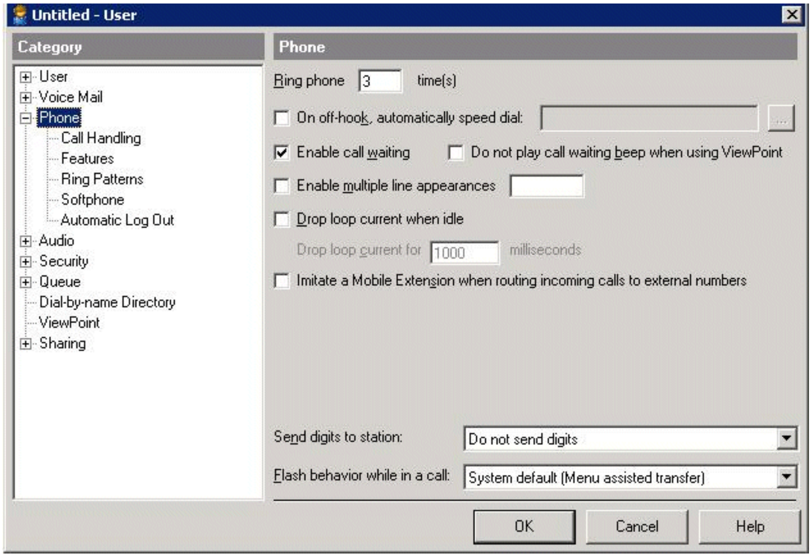
10 Click **OK** to return to the Cascading Notifications tab. When you click **OK**, a new cascading notification is added to the list of those that have been created so far. Cascading notifications will be performed in the order listed. Use the **Up** and **Down** arrows to rearrange the list order.

11 Select one of the following final actions to perform if all of the cascading notifications defined here have been sent and the voice message has still not been listened to:

- **Do nothing - stop notifying**.
- **Write an event to the event log**. Depending on how your Event Log is configured, this may result in a Wave system administrator being notified of the event via e-mail.
- **Move the message to the mailbox**. Select the voice mailbox where the voice message will be sent from the drop-down list. Note that depending on that voice mailbox owner’s own notification settings, another sequence of cascading notifications may be initiated.

The Phone tab

You use the Phone tab to configure basic options for the user’s phone. The options available on this tab vary depending on the phone type (analog, digital, or SIP). The following graphic shows the Phone tab for an analog phone user.



Phone

Ring phone 3 time(s)

□ On off-hook, automatically speed dial:

☑ Enable call waiting □ Do not play call waiting beep when using ViewPoint

□ Enable multiple line appearances

□ Drop loop current when idle

Drop loop current for 1000 milliseconds

□ Imitate a Mobile Extension when routing incoming calls to external numbers

Send digits to station: Do not send digits

Flash behavior while in a call: System default (Menu assisted transfer)

This section describes the following:

- Setting the number of rings for the phone. See page 11-59.
- Having the phone automatically dial when taken off hook. See page 11-59.
- Using call waiting. See page 11-60.
- Enabling multiple line appearances on an analog phone. See page 11-62.
- Dropping loop current when idle on an analog phone. See page 11-63.
- Using mobile extensions for externally routed calls. See page 11-63.

- Automatically going off-hook when alerting. See page 11-65.
- Sending digits to an analog phone. See page 11-65.
- Disabling softkeys on a digital phone. See page 11-66.
- Configuring Flash behavior on an analog phone. See page 11-67.

Setting the number of rings for the phone

This section applies to all phone types. (This option can also be set in ViewPoint.)

To set the number of rings for the user's phone

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone tab in the **Ring phone __ times** field, enter the number of times to ring the user's extension before proceeding to the next action in the user's routing list.

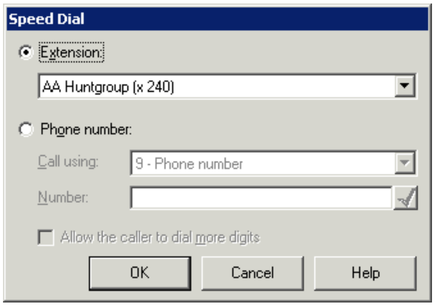
Having the phone automatically dial when taken off hook

This section only applies to digital and SIP phone users.

You can configure the user's phone to automatically dial a number whenever it is taken off hook, for example to create a lobby phone, waiting room phone, or hotline phone.

To have the user's phone automatically dial when taken off hook

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone tab, select the **On offhook, automatically speed dial** checkbox, and then click ... to open the Speed Dial dialog.



Speed Dial

● Extension:

AA Huntgroup (x 240)

○ Phone number:

Call using: 9 - Phone number

Number:

□ Allow the caller to dial more digits

3 Select one of the following:

- **Extension**. Select the extension to speed-dial from the drop-down list.
- **Phone Number.** Select this option to speed-dial an external number and/or access code. Enter the following information:
  - **Call using**. Select the dialing service for Wave to use to speed-dial the external number. You can also supply just the access code for an external call, so that the user can place external calls without having to dial the access code (see **Allow the caller to dial more digits** field, below).
  - **Number.** Specify the external number. If you supplied only the access code for an external call in **Call using** as described above, leave this field blank.
  - **Allow the caller to dial more digits**. Select this checkbox when you specify just an access code in the **Call using** field. This allows the user to place external calls without dialing the access code. Note that if you configure this feature this way, in order to dial an internal number from this phone, the user must pick up the phone and press Flash to get internal dial tone.

    Leave this checkbox unselected to automatically dial the **Number** as entered, without the user being able to enter additional digits.

Using call waiting

This section applies to all phone types.

To provide call waiting on the user's phone

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 On the Phone tab select the **Enable call waiting** checkbox.

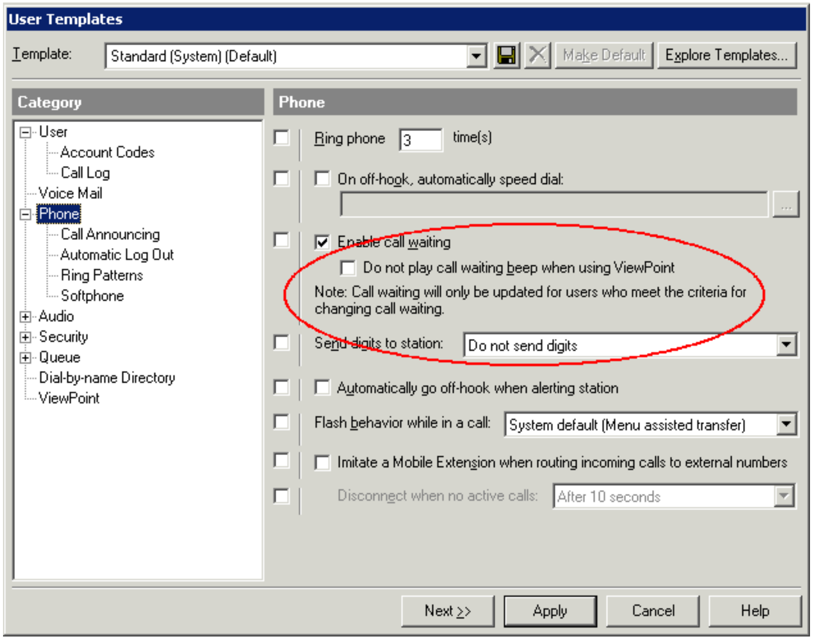
If unchecked, when the user is on a call new calls go straight to voicemail without playing the call waiting beep.

3 If the user uses ViewPoint's Call Monitor folder to spot incoming calls, and thus does not want the audible beep over the phone, check **Do not play call waiting beep when using ViewPoint.**

Note that the ability to enable the Call Waiting feature varies depending on phone type.

- **Analog phones**. By default, the **Enable call waiting** checkbox is selected and the **Do not play call waiting beep when using ViewPoint** checkbox is not selected.
- **Digital phones**. Both the **Enable call waiting checkbox** and the **Do not play call waiting beep when using ViewPoint** checkbox are disabled, until a Call Waiting feature button is configured on the phone. Then, the default settings are the same as for analog phones.
- **SIP phones**. Unless the SIP phone supports call waiting natively, neither checkbox appears in the User dialog. Currently only the 9112i and 51i SIP phones support call waiting natively. For these phones, the default settings are the same as described for analog phones.

Note: If you set call waiting options via a user template, the template may be applied later to a user whose phone type does not support call waiting. In this scenario, call waiting settings will not be applied to those users, as indicated by the note on the Phone tab of the User templates dialog:


User Templates

Template: Standard (System) (Default)

Category

Phone

□ Ring phone 3 time(s)

□ □ On off-hook, automatically speed dial:

□ ☑ Enable call waiting

□ Do not play call waiting beep when using ViewPoint

Note: Call waiting will only be updated for users who meet the criteria for changing call waiting.

□ Send digits to station: Do not send digits

□ □ Automatically go off-hook when alerting station

□ Flash behavior while in a call: System default (Menu assisted transfer)

□ □ Imitate a Mobile Extension when routing incoming calls to external numbers

□ Disconnect when no active calls: After 10 seconds

Enabling multiple line appearances on an analog phone

This section only applies to analog phone users.

You can use this option to give an analog phone user extra “lines” to handle simultaneous incoming calls. When the user is on a call and a new incoming call arrives on another line, the user hears the call waiting beep and can take the call by pressing Flash or via the ViewPoint Call Monitor. A user with active calls on multiple lines can switch between them using the Call Monitor or the phone commands, as described in the *Wave Phone User Guide*.

To enable multiple line appearances on an analog phone

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone tab, select the **Enable multiple call appearances** checkbox.
3. Enter the number of extra lines available to this user.

The **Enable multiple call appearances** and **Enable call waiting** checkboxes work in conjunction as follows:

- **Both checkboxes unselected**. The user has one line. If the user is on the phone, new incoming calls go straight to the next step on the user’s routing list. The user never hears a call waiting beep.
- **Enable call waiting selected, Enable multiple line appearances unselected**. Standard call waiting. The user has two lines, one for the current call, and one for the “call waiting” call. Once both lines are in use, new incoming calls go straight to the next routing list step with no call waiting beep.
- **Enable call waiting unselected, Enable multiple line appearances selected**. The user has the number of lines that you specify. When the user is on the phone, he or she hears the call waiting beep and can press Flash to accept incoming calls until all the lines are in use. Only when all the lines are in use do new incoming calls go straight to the next routing list step with no call waiting beep.
- **Both checkboxes selected**. The user has an infinite number of lines. New calls always trigger call waiting and never go straight to the next routing list step.

Dropping loop current when idle on an analog phone

This section only applies to analog phone users.

This option is useful if you have a third-party application that needs “disconnect supervision” to detect the moment a call ends, for example, an application that records voice messages. The end of a call causes an interruption of line current that third-party applications should respond to immediately.

To drop loop current when idle on an analog phone

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone tab, select the **Drop loop current when idle** checkbox to cause Wave to briefly interrupt current on the line whenever the user’s phone enters the Idle state (on-hook/not in a call). If unchecked, line current is maintained when the station enters the Idle state.
3. In **Drop loop current for ___ milliseconds**, enter the duration of current interruption. The default is 1 second (1000 milliseconds).

Using mobile extensions for externally routed calls

A Wave mobile extension allows a user’s remote phone to be treated as a Wave station. A remote phone is any phone that is external to the Wave system, for example a cell phone, home phone, iPhone, or legacy PBX phone.

Hint: Configuring a mobile extension according to the following steps is recommended (but optional) for an iPhone user using the ViewPoint Mobile App to ensure that calls forwarded to the user’s ViewPoint Mobile number also appear in the user's Call Log in ViewPoint.

With a mobile extension, a user at a remote phone can:

- Use ViewPoint to manage voice messages and greetings, place outbound calls, answer and handle calls displayed in the Call Monitor, and so forth. No configuration steps are required to enable this functionality for a user.
- Use ViewPoint to answer and handle calls that are forwarded to a remote phone or routed to a remote phone as a result of an action in the user’s routing list. You enable this feature for a user as described below.
- Use the Wave phone commands for full call control even if the user is not using ViewPoint.

Wave automatically creates a mobile extension in the following cases:

- When a user supplies a remote number when logging on to ViewPoint (as described in "Using ViewPoint with a different phone or Wave Server" in Chapter 2 in the *Wave ViewPoint User Guide*).
- When the **Imitate a Mobile Extension when routing incoming calls to external numbers** checkbox is selected for a user (as described below), a mobile extension is automatically created:
  - For each external number in the user's routing list.
  - When the user forwards his or her calls to an external number.

  When the user is currently logged on to ViewPoint at one of these numbers, incoming calls that are forwarded to or routed to the user's remote phone show up in ViewPoint and can be handled as Wave station calls. If the user is not currently logged on to ViewPoint when an incoming call comes in to one of these numbers, the user can press *# to access the phone commands to manage the call.

To create a mobile extension when routing incoming calls to the user

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone tab, select the **Imitate a Mobile Extension when routing incoming calls to external numbers** checkbox to enable ViewPoint call handling features on calls forwarded or routed to a user at a remote phone.

   If deselected, calls forwarded or routed to a user at a remote phone do not appear in the ViewPoint Call Monitor.
3. Select one of the following from the **Disconnect when no active calls** drop-down list to specify how long to wait before disconnecting a mobile extension when there are no active calls.
   - **Immediately**
   - **After 5 seconds**
   - **After 10 seconds**. This is the default setting.
   - **After 15 seconds**
   - **After 30 seconds**
   - **When Mobile Extension hangs up**

This setting specifies the number of seconds of dial tone played to the user of a mobile extension after the remote party disconnects, or when the mobile extension user disconnects a call in ViewPoint. You can set the mobile extension disconnect for an individual user or at the user template level.

Automatically going off-hook when alerting

This section only applies to digital and SIP phone users.

This setting is disabled by default for digital and SIP phone users.

- When this setting is enabled, the user’s phone automatically goes off-hook when the user selects a ViewPoint feature that uses the phone, such as play audio or place a call.
- When this setting is disabled, the phone rings normally if it is on-hook when the user selects a ViewPoint feature that uses the phone.

To automatically go off-hook when alerting

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone tab, select the **Automatically go offhook when alerting station** checkbox to have the station automatically go off-hook when the user selects ViewPoint features that use the phone, such as play audio or place a call.

   If unchecked, the phone rings normally if it is on-hook when the user selects these ViewPoint features.

Sending digits to an analog phone

This section only applies to analog phone users.

If you are integrating a third-party device with Wave, such as a fax server or voice mail system, you may need to indicate how to send DID information to the station as touch tone digits (DTMF). Consult the documentation that came with your third-party device for more information about the kind of DTMF information that is required.

To send digits to an analog phone

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone tab, select one of the following options:
   - **Do not send digits**. Select this method (the default) if you are not integrating a third-party device. No DTMF digits are sent.
   - **Send DID from PSTN**. Send the DID number as DTMF digits from the trunk on which the call came in
   - **Send user's extension number**. Send the extension number of the calling user as DTMF digits.
   - **Send call type and extension number**. Send the call type and extension number as DTMF digits.

If you choose any setting except **Do not send digits** (the default), all call screening options are disabled for the station.

Disabling softkeys on a digital phone

This section only applies to digital phone users.

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone tab, select the **Disable Softkeys** checkbox to disable the softkeys used to make selections from the display screen on a digital phone.

Configuring Flash behavior on an analog phone

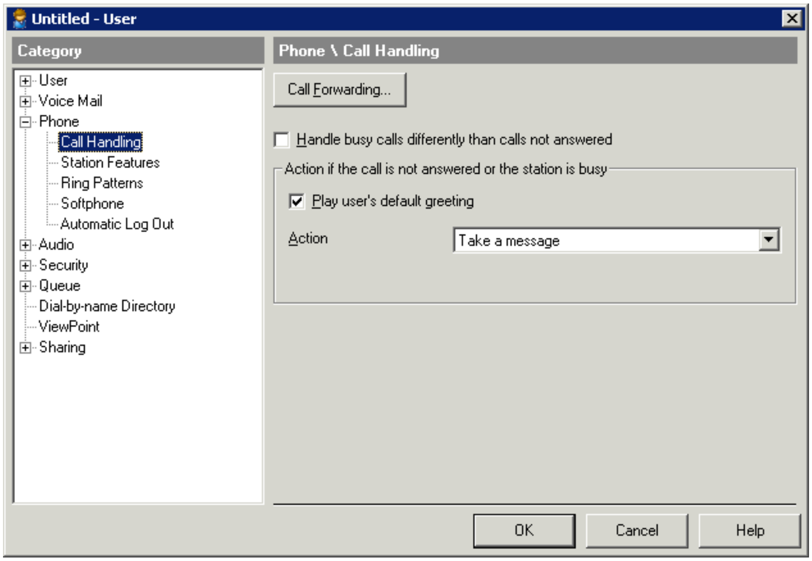
This section only applies to analog phone users.

You can use the **Flash behavior while in a call** field on the Phone tab to select what happens when this user presses Flash (or quickly presses the hook) while on a call. The options are as follows:

- **System default**. The user’s behavior is whatever you have chosen as the system-wide behavior. (See “Setting general options” on page 4-4.)
- **Menu assisted transfer**. Pressing Flash takes the user to a menu giving you options for transferring the call.
- **Direct transfer**. Pressing Flash lets the user immediately enter an extension to transfer the call. Choose this option to make transfers faster and simpler for a user who answers and transfers many calls. Note that with direct transfer, the user cannot access Conference or the other commands on the call handling menu unless he or she has ViewPoint.
- **Manage current call**. Pressing Flash takes the user to the Wave call handling menu, of which one of the options is transferring the call (for details, see Appendix A of the *Wave ViewPoint User Guide*).

The Phone \ Call Handling tab

Use the Phone \ Call Handling tab to forward a user’s calls and configure how incoming calls are handled if the user’s line is busy or the call is not answered.



□ Handle busy calls differently than calls not answered

Action if the call is not answered or the station is busy

☑ Play user's default greeting

Action: Take a message

Note: Changing the settings on this tab may alter the user's Preferred Location in their Standard routing list.

This section describes the following:

- Configuring actions for unanswered or busy calls. See page 11-69.
- Forwarding the user’s calls. See page 11-71.

Configuring actions for unanswered or busy calls

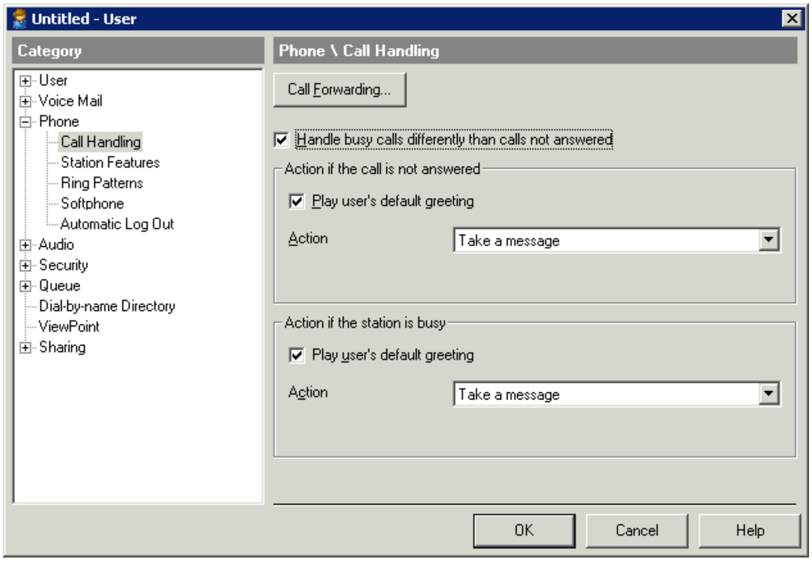
Use the fields in the **Action if the call is not answered or the station is busy** section of the Phone \ Call Handling tab to specify what happens when the user receives an incoming call that goes unanswered or that is received while the user's phone is off-hook.

The available actions are:

- **Take a message**. The call is sent to the user's voicemail.
- **Transfer to external number.** The call is transferred to the external number you enter in the **Number** text box.
- **Transfer to extension**. The call is transferred to the Extension you select from the **Extensions** drop-down list, for example, an operator, a co-worker who handles the user's calls, or an auto attendant. The transferred call is treated as a new call to that extension. If no one answers at that extension, the call follows that extension's routing list.
- **Transfer to other voicemail.** The call is transferred directly to the voicemail of the extension you select from the **Mailbox** drop-down list.
- **Hang Up.** The call is disconnected.

Optionally, you can also select the **Play user's default greeting** checkbox for either action to play the user's default greeting before performing the action specified.

By default, the same action is applied to both types of calls. To select a different action for unanswered vs. busy calls, select the **Handle busy calls differently than calls not answered checkbox**.



Untitled - User

Phone \ Call Handling

☑ Handle busy calls differently than calls not answered

Action if the call is not answered

☑ Play user's default greeting

Action: Take a message

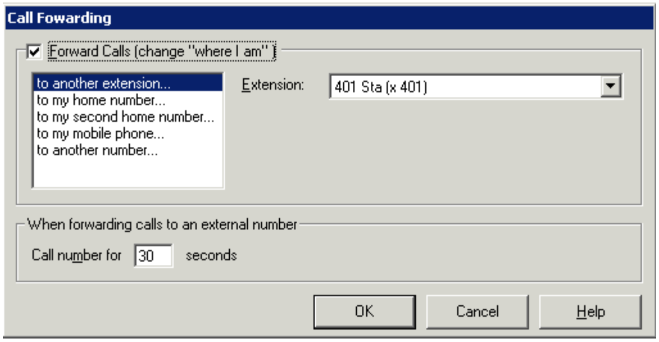
Action if the station is busy

☑ Play user's default greeting

Action: Take a message

Forwarding the user’s calls

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone \ Call Handling tab, click **Call Forwarding** to forward the user’s calls. The Call Forwarding dialog opens.



Call Fowarding

☑ Forward Calls (change "where I am")

Extension: 401 Sta (x 401)

When forwarding calls to an external number

Call number for 30 seconds

3. Select the **Forward calls** checkbox.
4. Select the type of forwarding destination in the list below.
5. Enter the forwarding extension or phone number. For external numbers, select the dialing service to use from the **Call Using** drop-down list.
6. Optionally, use **Call number for __ seconds** to determine how long a call rings at the forwarded phone before proceeding to the next step on the user’s routing list (usually voicemail).

Call forwarding and voicemail

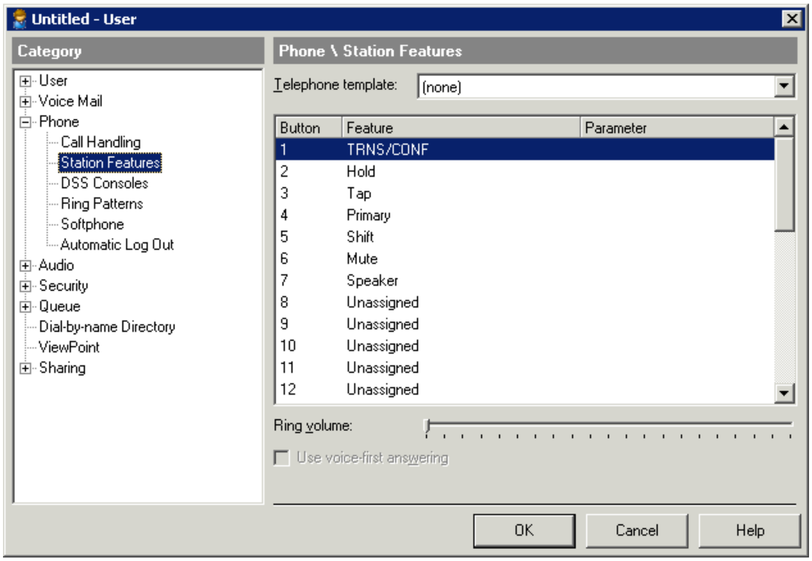
If a forwarded call is not answered, it is sent to the user’s voicemail.

To completely transfer a user’s calls to another user's phone, so that the other user receives voicemail as well as the calls themselves, do not use call forwarding. Instead, use ViewPoint to create a routing list whose final (and only) action is Transfer to Extension, and make it the user’s active routing list. See the *Wave ViewPoint User Guide*.

The Phone \ Station Features tab

Use the Phone \ Station Features tab to configure the special features that are available on the user’s phone.

Note: Some features are available only for digital or SIP phones.



Untitled - User

Category: User, Voice Mail, Phone (Call Handling, Station Features, DSS Consoles, Ring Patterns, Softphone, Automatic Log Out), Audio, Security, Queue, Dial-by-name Directory, ViewPoint, Sharing

Phone \ Station Features

Telephone template: (none)

Button	Feature	Parameter
1	TRNS/CONF	
2	Hold	
3	Tap	
4	Primary	
5	Shift	
6	Mute	
7	Speaker	
8	Unassigned	
9	Unassigned	
10	Unassigned	
11	Unassigned	
12	Unassigned	

Ring volume:

□ Use voice-first answering

The Phone \ Station Features tab has the following options:

- **Phone template**. To apply a pre-selected slate of features from a template, select the template from the drop-down list. For more about templates, see “Configuring phone templates” on page 10-2.

  Note: For analog phone users, **Phone template** is the only field available on this tab, which is called Features.

- **Button list**. For a digital or IP phone, the central pane of the dialog shows a list of features currently assigned to feature buttons on the phone.

To assign or change a feature assigned to a feature button

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the Phone \ Station Features tab.
3. Click in the **Feature** column for the button, and then click the arrow icon that appears.
4. Select the feature to assign from the drop-down list.

   Note: You must first create a trunk group with outside lines enabled (via the Trunks Group applet) before the Outside Line option will be presented in the list of features that can be configured for a digital phone.

5. Some features have additional settings. Click in the **Parameter** column for the button, and then click the "..." icon if one appears.
6. Specify the required and optional settings as needed in the dialog that opens.
7. Click **OK** to save your changes.
8. Drag the slider bar to adjust the **Ring volume** of the phone.
9. Select the **Use voice-first answering** checkbox to enables voice-first answering. With voice-first answering, internal calls are connected to the user's speakerphone automatically without the phone ringing or needing to be picked up. All external calls ring the phone as normal.

The Phone \ DSS Consoles tab

Note: This tab is displayed only if you specified a digital phone type that supports the DSS Console (see "The User tab" on page 11-15.) In this version, the DSS console is only supported on the Edge 700 series digital phones.

You use this tab to configure one or more DSS Console devices associated with a user's digital phone. A DSS console provides "switchboard" capability by expanding the number of extension buttons available to a digital phone user.

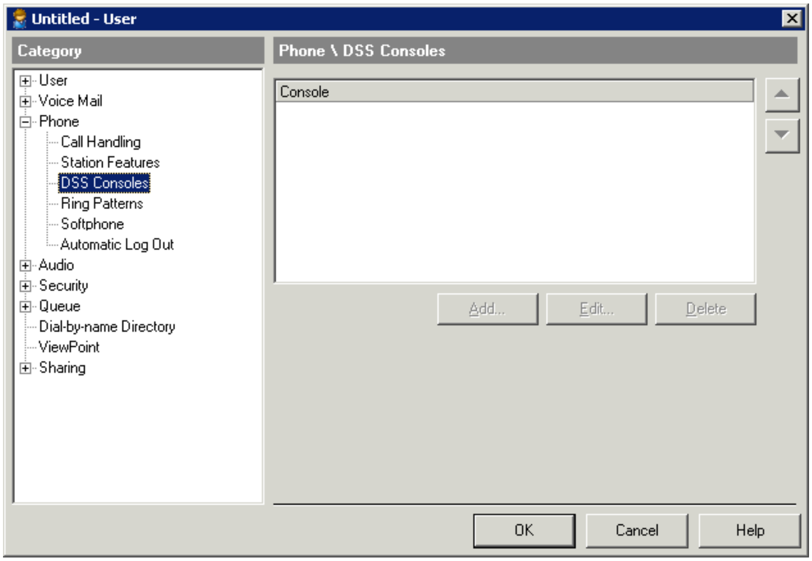
The DSS Console expands a receptionist's digital phone with 48 additional flexible buttons with LEDs to connect to system endpoints such as user extensions. Up to 5 DSS Consoles can be associated with a single digital phone, providing up to 240 additional buttons.

You can assign most of the same features to a DSS Console button that you can assign to a button on the user's digital phone. Typically, you assign a Line Appearance feature button for each extension for which this user will answer calls via this DSS console.

Note the following:

- Feature button configuration restrictions are enforced across the user's digital phone and all associated DSS Consoles, for example a restriction that states you can configure only one button of the same type for a user vs.multiple buttons of the same type.
- The following features cannot be assigned to a button on the DSS Console - these features can only be assigned to a button on the user's digital phone:
  - Primary
  - Program
  - Shift
  - Speaker
  - Tap

See "The Phone \ Station Features tab" on page 11-72 for a description of each feature, as well as required and optional settings, configuration restrictions, and so forth.



Important! If you change the user’s **Telephone type** via the User tab while one or more DSS consoles are connected to that extension, a message warns you if DSS consoles are not supported on the new phone type, or if the number of DSS consoles already configured for this user will be over the limit supported on the new phone type. Also, the DSS console button configurations for those DSS Consoles will be deleted, and you will have to redefine all of the buttons, as described below. This limitation will be addressed in a future version.

For instructions on how to connect a DSS Console on the Wave Server, see Chapter 4 in the *Wave Server Installation Guide*.

DSS consoles and extensions are included in some of the reports available via the Report Generator applet.

- **Station Ports report**. DSS console extensions are listed in the **Primary Extension** column using the format “<Extension> DSS <n>”, for example “105 DSS 1”.
- **Phone Button report**.

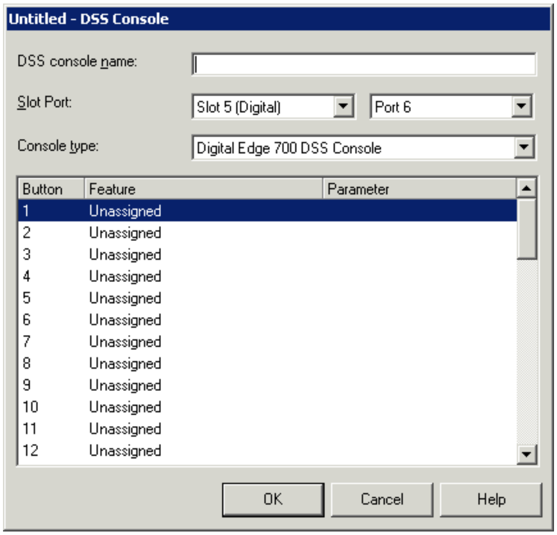
DSS console extensions are also listed in the Station Ports applet. However, they are not listed in the Station Monitor applet, which only lists the user’s primary extension.

To add a DSS console to a user’s digital phone configuration

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 Click the Phone \ DSS Consoles tab.

3 Click **Add** to add a new DSS console or **Edit** to modify the selected one. The DSS Console dialog opens:



Untitled - DSS Console

DSS console name:

Slot Port: Slot 5 (Digital) Port 6

Console type: Digital Edge 700 DSS Console

Button	Feature	Parameter
1	Unassigned	
2	Unassigned	
3	Unassigned	
4	Unassigned	
5	Unassigned	
6	Unassigned	
7	Unassigned	
8	Unassigned	
9	Unassigned	
10	Unassigned	
11	Unassigned	
12	Unassigned	

Note: The **Add** button is disabled if you have already configured the maximum number of DSS consoles for this user’s phone type.

4 Enter the following information for this DSS console:

- **DSS console name**. Enter a descriptive name for this DSS Console. DSS console name can be maximum of 30 characters. Spaces, special characters, and numbers are allowed.
- **Slot Port**. Select the appropriate slot and port for the DSS console from the drop-down lists.
  - **Slot**. Defaults to the same slot assigned to the user’s digital phone (see “The User tab” on page 11-15.)
  - **Port**. Defaults to the next available port on that slot.
- **Console type**. Select the DSS console model type from the drop-down list. In the current version, only one console type is supported, “Digital Edge 700 DSS Console”.

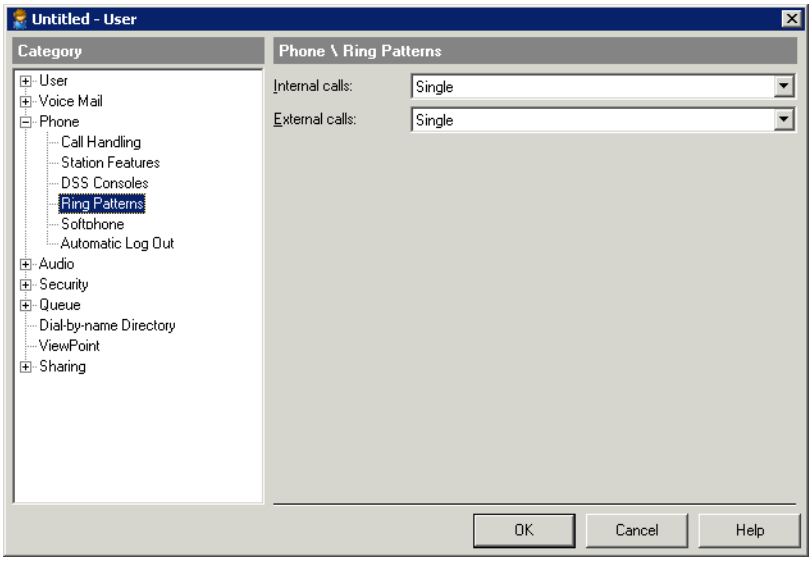
5 All of the feature button assignments for this DSS console are listed in the bottom pane. To assign a feature to an unassigned button, click in the **Features** column for that button, and then select the feature from the drop-down list.

6 Some features have additional settings. Click in the **Parameter** column for the button, and then click the "..." button if one is available. Specify the required and optional settings as needed in the dialog that opens.

7 Click **OK** until you return to the DSS Consoles tab.

The Phone \ Ring Patterns tab

You use this tab to configure different ring tones for internal and external calls.



Internal calls: Single

External calls: Single

To configure ring patterns

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

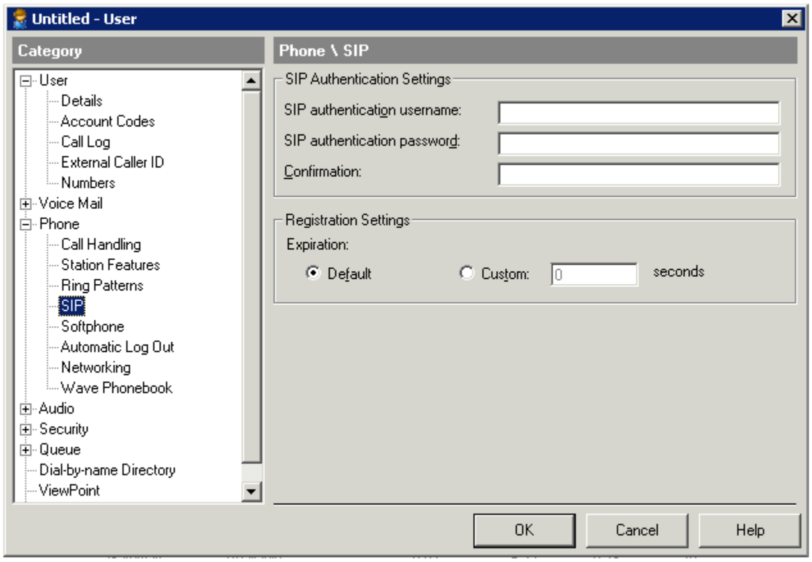
2 Click the Phone \ Ring Patterns tab.

3 Select a ring pattern (**Single**, **Double**, or **Triple**) for **Internal calls** from the drop-down list.

4 Do the same for **External calls**.

The Phone \ SIP tab

You use this tab to specify SIP authentication and registration settings for a user.



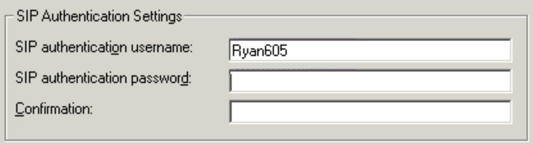
This section only applies to SIP phone users.

SIP authentication passwords are different from regular Wave passwords, and are not affected by the password settings described in “Enforcing strong password security” on page 4-14.

Note: See “Setting up SIP endpoint authentication” on page 6-10 for other configuration steps you must complete in order to perform SIP authentication with Wave.

To specify SIP authentication and registration information for a user

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. On the Phone \ SIP tab in the SIP Authentication Settings section, the user’s **SIP authentication username** is assigned automatically and cannot be changed. **SIP authentication username** consists of the user’s last name plus extension.



SIP Authentication Settings

SIP authentication username: Ryan605

SIP authentication password:

Confirmation:

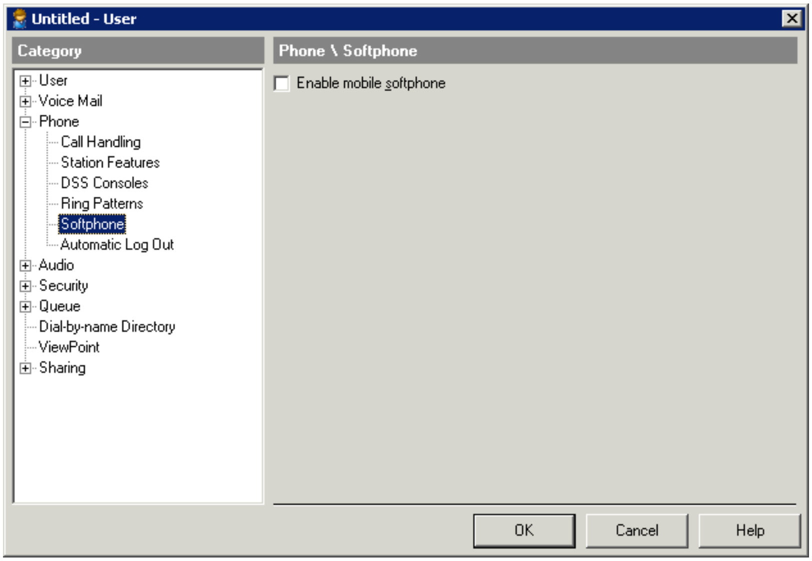
3. Enter the user’s **SIP authentication password**, and then re-enter it in the **Confirmation** field. This password can be a maximum of 48 characters, and can include alphanumeric characters, spaces, and special characters. A blank password is allowed.
4. In the Registration Settings section, specify the length of time in seconds before a SIP phone or SCP attempts to reregister.

   Use the default value unless you want to specifically override the default global registration expiration timer for this user.

   - **Default**. Use the default global registration expiration timer value specified via IP Telephony in the SIP Advanced Parameters dialog.
   - **Custom**. For this user, specify the number of seconds to use for the registration expiration timer.

The Phone \ Softphone tab

You use the Softphone tab to enable the user to use the ViewPoint Softphone.



□ Enable mobile softphone

With the ViewPoint Softphone, a user can dial numbers via the ViewPoint Softphone dial bar and answer calls via the Call Monitor. The ViewPoint Softphone uses the PC’s microphone and speakers, headset, or other USB audio devices for audio playback and capture.

The ViewPoint Softphone can be used in either of the following ways:

- **As a primary phone**, when a user does not have a physical phone. The ViewPoint Softphone can be used as a user’s primary phone from the local LAN or when running ViewPoint while logged in via VPN from a remote location. One Wave IP User license is required for each user who uses the ViewPoint Softphone as his or her primary phone.
- **As as a secondary phone**, allowing a user to place and take calls via ViewPoint when the user is away from his or her physical phone. No additional Wave licenses are required for users who use the ViewPoint Softphone as a secondary phone—usage of the ViewPoint Softphone is covered by those users’ existing Wave ISM User licenses.

Before you can enable the ViewPoint Softphone for a user via this tab, the following requirements must be met:

- Specify the user's phone type as described in "Specifying a phone type and model" on page 11-17.
- Make sure that adequate Wave licenses are available on the Wave Server. When the ViewPoint Softphone is used as a primary phone, a Wave IP User license is required for that user. When the ViewPoint Softphone as a user's secondary phone, no additional Wave license is required—usage of the ViewPoint Softphone is covered by the user's existing Wave ISM User license.

To enable the ViewPoint Softphone

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the Phone \ Softphone tab.
3. Select the **Enable mobile softphone** checkbox. (This checkbox is disabled if no Wave ISM User license is available, or you have not yet specified the user's phone type on the User tab.)

   When you save a user with this checkbox selected, an extension is automatically assigned with the format "Vnnnnnn". This extension will inherit the user's properties, except for the following:

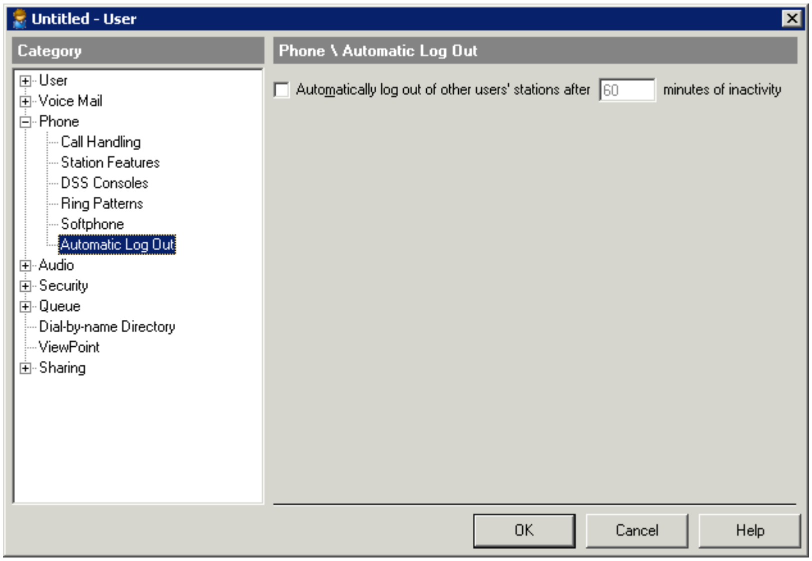
   - No folders, permissions, routing lists, or other features are associated with this extension.
   - This extension is not displayed in any lists of user extensions in ViewPoint.
   - This extension is not listed in the dial-by-name directory.

   Note: This extension is only used internally by Wave. Other users and external callers will still "know" this user by his or her regular Wave extension.

4. Once this option is enabled, in order for the user to use the ViewPoint Softphone, configure the audio playback and capture devices on the user's laptop in ViewPoint by choosing **Tools > Options > Phone > Softphone Devices**. For more information, see Chapter 12 in the *Wave ViewPoint User Guide*.

The Phone \ Automatic Log Out tab

You use this tab to enable and configure the automatic log out feature for a user.



□ Automatically log out of other users' stations after 60 minutes of inactivity

Note: This tab applies to all phone types—analog, digital, and SIP.

If the user has logged in at another user’s workstation—using either ViewPoint or the phone commands—the setting on the User dialog’s Phone \ Automatic Log Out tab determines how much inactive time elapses before the user is automatically logged out and the station is reset to its default user. This feature is useful if a roaming user walks away from a phone without logging out.

To specify the automatic logout interval

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the Phone \ Automatic Logout tab.
3. Enter the number of minutes in **Automatically log out of other user’s stations after __ minutes of inactivity**.

All calls are written to the Call Log according to the user logged in at the station, so a user can log in anywhere in the office and make calls that are logged correctly under his or her name. Calls from the station continue to be logged under the visiting user’s name until one of the following happens:

- The visiting user logs out, either by pressing ***000** at the dial tone if the user used ***51** to forward his or her calls or by choosing **File > Exit and Log Off** in ViewPoint. This resets the station to its default user.
- Another user logs in to the station using ViewPoint or phone commands. This resets the station to the new user.
- The amount of time specified in **Automatically log out of other user’s stations after __ minutes of inactivity** is exceeded. This resets the station to the default user. Inactivity is defined as any time except during active calls (inbound or outbound) and when phone commands are used that require entering a password (for example, logging into the phone to listen to voicemail). All other station activity, such as picking up the phone and dialing *14, or using ViewPoint to play a voice message over the station, count as inactivity.

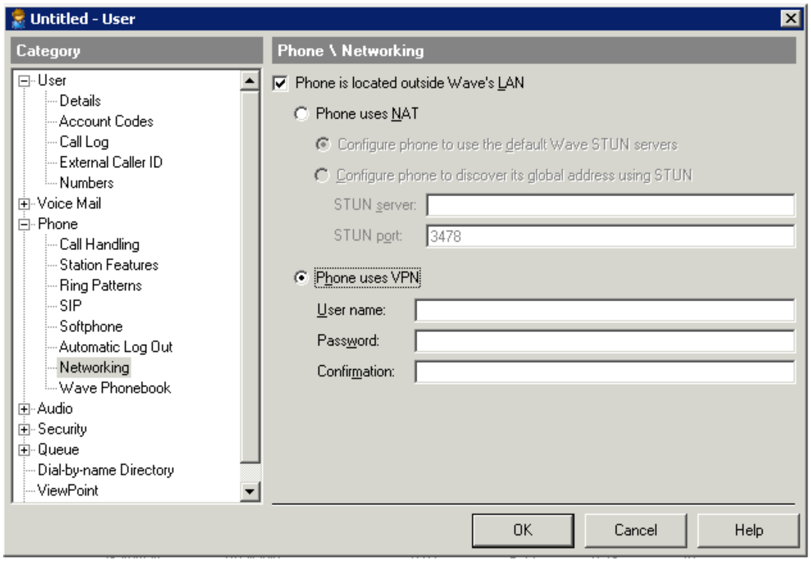
Note: Incoming calls for other users, such as calls forwarded to the station, do not count as activity even if they are answered.

Deselect the **Automatically log out of other user’s stations after __ minutes of inactivity** checkbox to prevent resetting the station after any amount of inactivity.

The Phone \ Networking tab

You use this tab to set up OpenVPN Server or NAT traversal for a SIP phone user. For details, see:

- “Setting up OpenVPN Server for a Wave Gigabit-E SIP phone user” on page 6-35
- “Setting up NAT traversal for a user” on page 6-37



☑ Phone is located outside Wave's LAN

○ Phone uses NAT

● Configure phone to use the default Wave STUN servers

○ Configure phone to discover its global address using STUN

STUN server:

STUN port: 3478

● Phone uses VPN

User name:

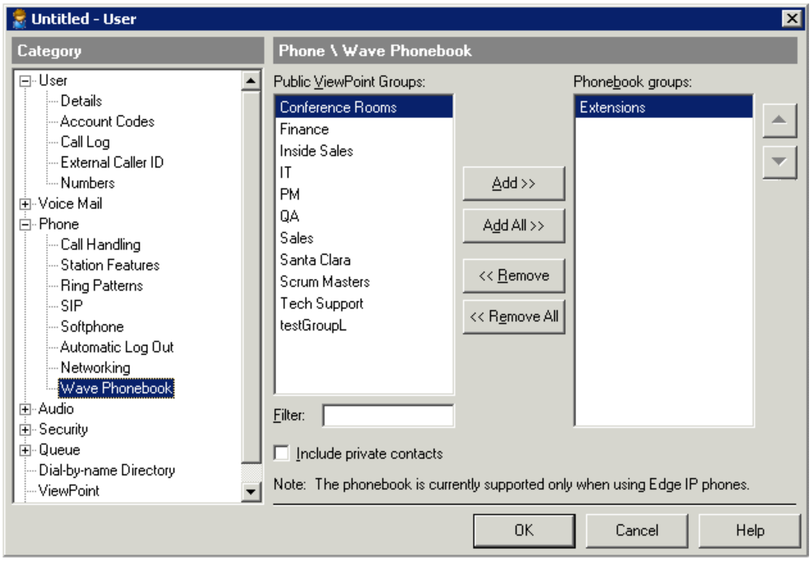
Password:

Confirmation:

The Phone \ Wave Phonebook tab

You use this tab to configure the Wave Phonebook for an Edge 5000i IP phone user.

The Wave Phonebook is a searchable directory of public ViewPoint Groups or private contacts that is accessible directly from a button on a user’s Edge 5000i IP phone. Especially for users with no access to ViewPoint, this feature provides access to the same synchronized directory information as other Wave users have, and makes deploying custom phonebooks (for example customer contact directories) easy to deploy.



Note: The phonebook is currently supported only when using Edge IP phones.

Setting up the Wave Phonebook for an Edge 5000i IP phone user consists of the following steps:

- Specifying the public ViewPoint Groups to appear in the user’s Phonebook.
- Adding a Phonebook button to the user’s Edge 5000i P phone

Using the Phonebook on an Edge 5000i IP phone is described in the *Wave Phone User Guide*.

To configure the Wave Phonebook for an Edge IP phone user

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 Click the Phone \ Wave Phonebook tab.

3 Use the **Add** and **Remove** buttons to build the Phonebook from the list of public ViewPoint Groups.

4 Select a Group in the Phonebook groups list and use the **Up** and **Down** arrow buttons to control the order in which the Groups will be displayed in the Phonebook on the user's phone.

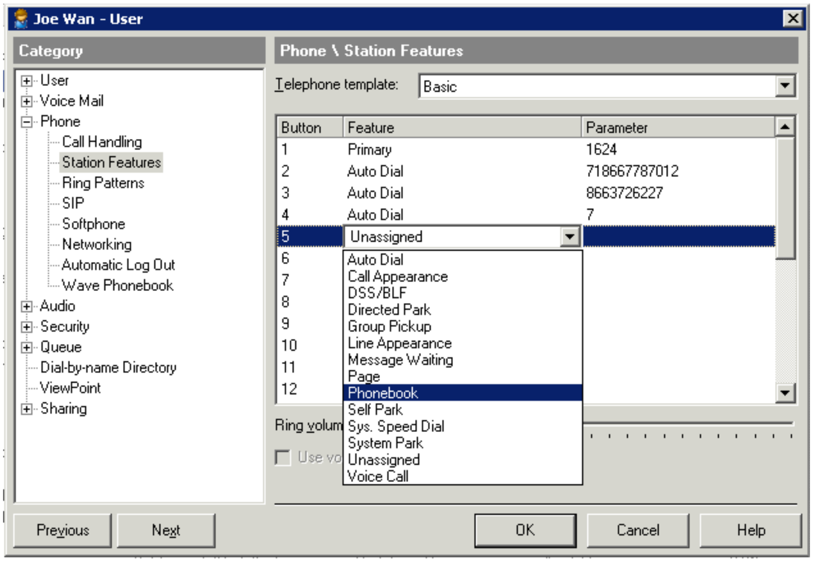
You can type into the **Filter** text box to quickly narrow the list of ViewPoint Groups, rather than having to scroll through the entire list.

5 Select the Include private contacts checkbox to include the phone's logged-in user's private contacts in the Phonebook directory. They will be listed in a "Private Contacts" group at the bottom of the Phonebook.

To add a Phonebook button on an Edge 5000i IP phone

1 In the User dialog, select Phone \ Station Features in the left pane

2 Assign the Phonebook feature to an unassigned button..



Joe Wan - User

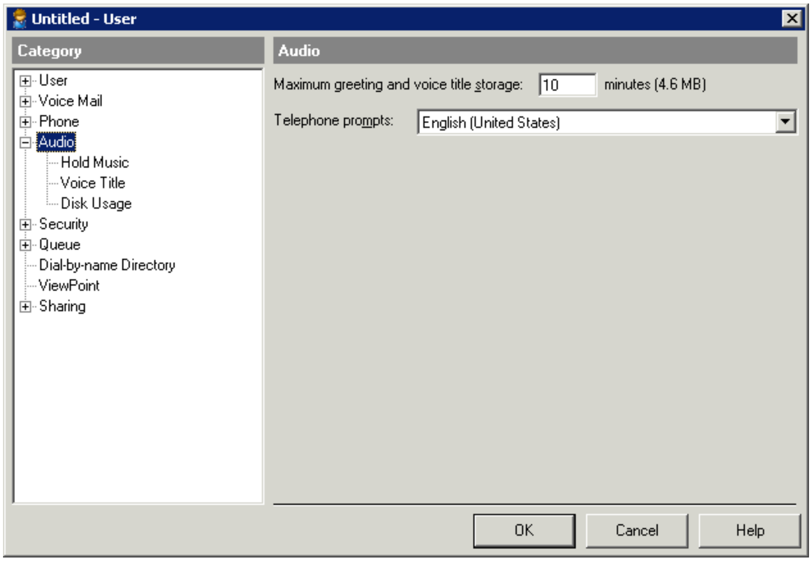
Phone \ Station Features

Telephone template: Basic

Button	Feature	Parameter
1	Primary	1624
2	Auto Dial	718667787012
3	Auto Dial	8663726227
4	Auto Dial	7
5	Unassigned	
6		
7		
8		
9		
10		
11		
12		

The Audio tab

You use this tab to allocate audio resources for the user.



Maximum greeting and voice title storage: 10 minutes (4.6 MB)

Telephone prompts: English (United States)

This section describes the following:

- Setting the storage size for greetings and voice titles. See page 11-89.
- Choosing a language for phone prompts. See page 11-89.

Setting the storage size for greetings and voice titles

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the Audio tab.
3. In the **Maximum greeting and voice title storage** field, enter how many minutes worth of audio files this user can store for greetings and voice titles. These voice file types include the following:
   - **Greetings**. All greetings displayed in ViewPoint's Greetings view.
   - **Voice titles**. The user's own voice title plus all voice titles for the user's contacts.

   The default setting of 10 minutes requires 4.6 MB of storage. The User/Group Management applet opens a warning message if the total allotment of voice message and greeting space for all users exceeds the available disk space on the Wave Server.

Choosing a language for phone prompts

From the **Telephone prompts** drop-down list, choose the language that Wave system prompts will play in for this user. When the user logs on or is identified on the phone, Wave automatically switches to this language for all subsequent system prompts during the call. The language can be also be set in ViewPoint. This setting does not affect any prompts that other callers or users hear.

The **Telephone prompts** drop-down list shows all of the languages currently installed on the Wave Server. See "Setting up system-wide audio options" on page 4-18 for more about how to install additional languages.

The Audio \ Hold Music, Voice Title, and Disk Usage tabs

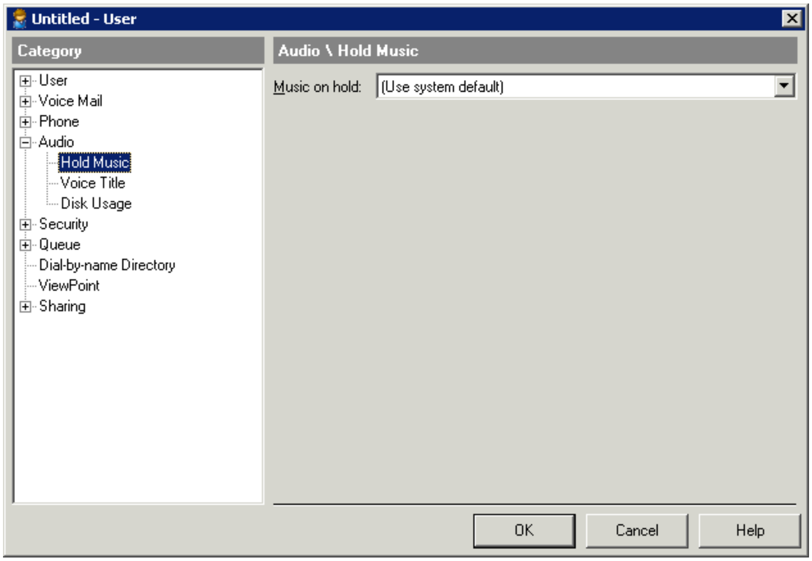
Expand the Audio tab category to select the Audio \ Hold Music, Audio \ Voice Title, and Audio \ Disk Usage tabs.

This section describes the following:

- Setting the user's hold music. See page 11-90.
- Recording the user's voice title. See page 11-92.
- Viewing the user's disk usage. See page 11-93.

Setting the user's hold music

Expand the Audio tab in the category pane to select the Hold music tab. You use this tab to configure a music-on-hold source for the user.



Music on hold: (Use system default)

Each user can have his or her own music-on-hold source as described below, or default to the system source (see "Configuring Music On Hold" on page 16-21.)

A caller hears this music while on hold for the user and continues to hear it while on hold until reaching a part of Wave that uses different hold music, such as a Contact Center queue or an auto attendant that has different hold music settings.

To customize hold music for a user

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the Audio \ Hold Music tab.
3. Expand the Audio tab category and select the Hold Music tab.

4 Select the **Music on hold** source you want to use for this user from the drop-down list.

- **(Use system default)**. Use the system-wide hold music source as specified in the General Settings applet.
- **Disabled**. Do not play music to callers on hold.

  Hint: It is highly recommended that you specify a music-on-hold source or use the system default so that a caller does not hear extended ringing or silence, which may result in a hang-up.

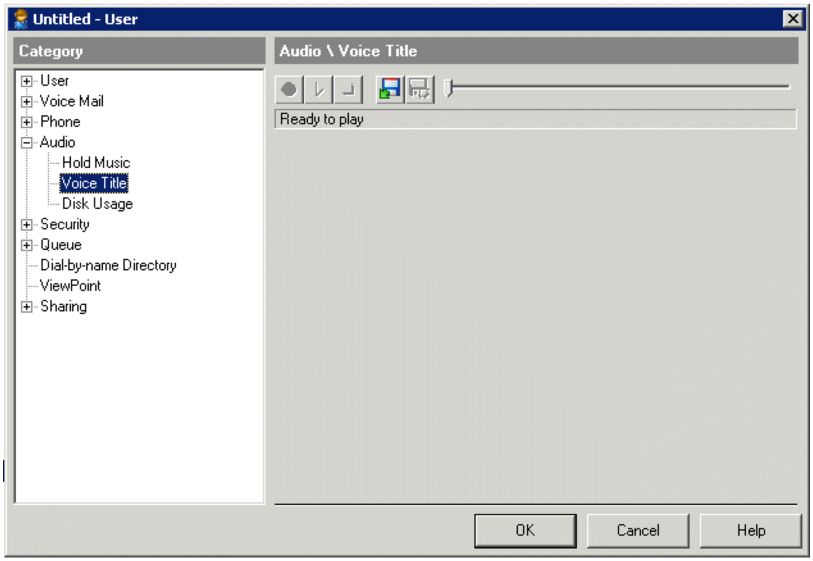
- **External (Audio Input Jack)**. Play hold music from an external device, typically a CD player, radio, or specialized music-on-hold device. This source is specified via the General Settings applet (PBX tab) in the Global Administrator Management Console. See “Configuring Music On Hold” on page 16-21.
- **Song n (<song title>)**. Play the selected WAV file to callers on hold.

Note: The system default music-on-hold source (if specified) as well as the other items listed in this drop-down list are set up via the General Settings applet. For more information, see “Configuring Music On Hold” on page 16-21.

5 Click **OK**.

Recording the user's voice title

Expand the Audio tab in the category pane to select the Voice Title tab. You use this tab to record the user's voice title.



A user's voice title is a short recording consisting only of the user's name. Wave uses the voice title in several prompts, for example, the call screening prompt when the user calls another user (the user receiving the call hears "Call from <voice title>"). Users can record their voice titles themselves in their own voices, using either the phone commands or ViewPoint. However, since the voice title is a critical part of the Wave system (for example, users without a voice title are not listed in the dial-by-name directory), it is recommended that you record them, after which those users who want to re-record them can do so.

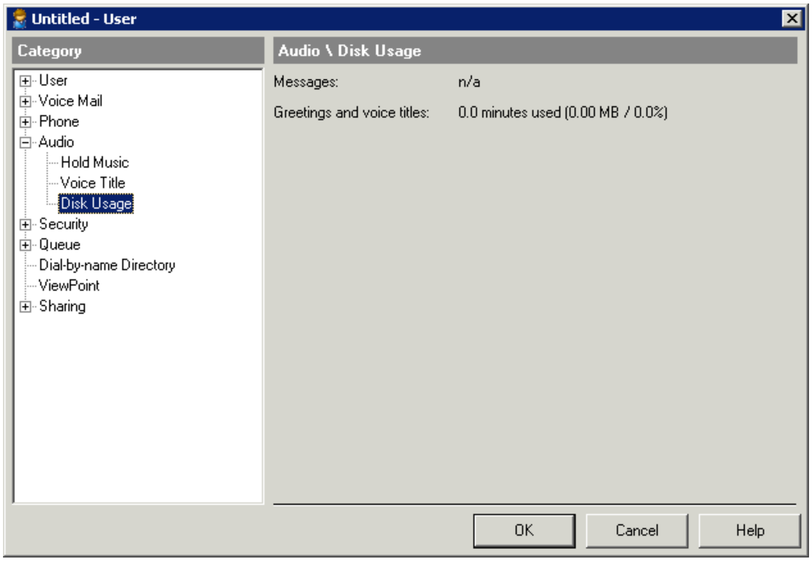
To record the voice title, use the audio controls. See "Using the audio controls" on page 2-21.

Viewing the user’s disk usage

1 In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.

2 Click the Audio \ Disk Usage tab.

3 Expand the Audio tab in the category pane to select the Disk Usage music tab. You use this tab to display how much space the user’s audio files are taking up. The percentage of allocated space is also displayed.



Untitled - User

Audio \ Disk Usage

Messages: n/a

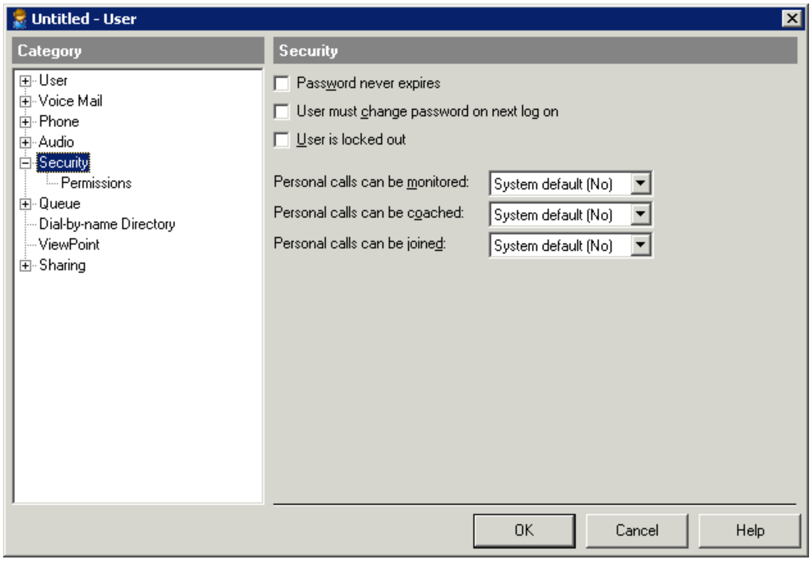
Greetings and voice titles: 0.0 minutes used (0.00 MB / 0.0%)

To avoid slowing the opening and scrolling of the Users view, Wave does not dynamically recalculate these totals. Totals are recalculated once a day at 1:00 a.m. You can also recalculate the totals at any time by choosing **Tools > Recalculate Disk Usage**.

To configure space for the user’s voice messages, see “The Voice Mail tab” on page 11-28. To configure space for the user’s greetings and voice titles, see “The Audio tab” on page 11-88.

The Security tab

You use the Security tab to configure the user's password settings and whether the user's calls can be supervised.



☐ Password never expires

☐ User must change password on next log on

☐ User is locked out

Personal calls can be monitored: System default (No)

Personal calls can be coached: System default (No)

Personal calls can be joined: System default (No)

This section describes the following:

- Configuring password expiration. See page 11-94.
- Configuring whether the user's calls can be supervised. See page 11-95.

Configuring password expiration

Use the options on the Security tab to protect the user's account and your Wave system from unauthorized access and toll fraud. For more information about toll fraud, see Appendix Appendix A.

The following security options are available:

- **Password never expires**. If checked, the user's password does not expire, although you can always manually change it or force the user to change it. If unchecked, the user's password may expire as determined by your system settings.

Note the following:

- Checking this field is a security risk, as long-standing passwords are easier to guess.
- You should check this field for users of IP phones that use PLAR, because a changed password prevents the phone from working.

- **User must change password on next logon**. If checked, the system requires the user to change his or her password the next time he or she logs on to any workstation application or by using the phone commands.
- **User is locked out**. If checked, the account cannot log on to the system, even with the correct username and password. Depending on your system settings, lockout can occur automatically if someone repeatedly tried and failed to log on to the account. Uncheck the field to unlock the account and permit normal logging on.

Configuring whether the user’s calls can be supervised

You can choose whether the user’s personal calls can be supervised by other users with permission to do so. These settings do not apply to Contact Center queue calls. Supervision of Contact Center queue calls is controlled separately by agent permissions.

In each of the following fields choose “Yes,” “No,” or “System Default”:

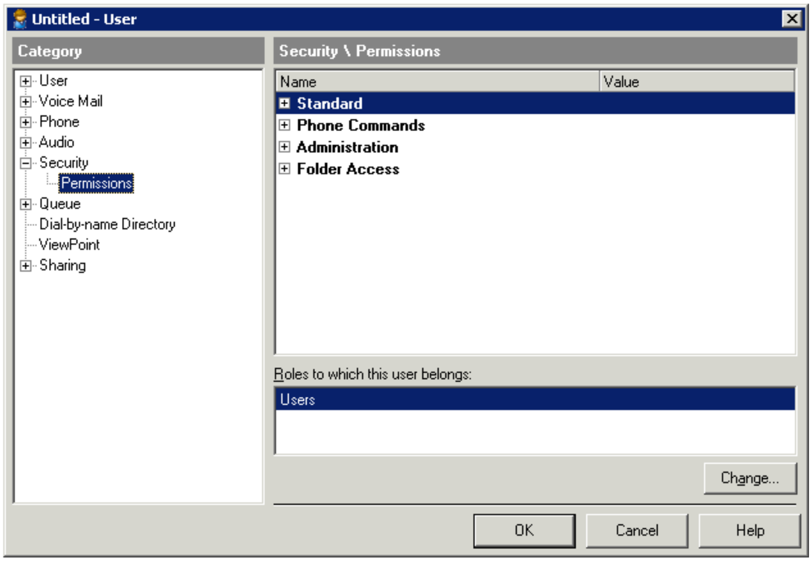
- **Personal calls can be monitored**. Any user with the “Allow monitoring user calls” permission can listen to this user’s personal (not queue) calls without this user knowing.
- **Personal calls can be coached**. Any user with the “Allow coaching user calls” permission can add himself or herself to this user’s personal (not queue) call and be heard by this user, but not by the caller.

  Note: To coach a call between two users, the user being coached must allow coaching *and* the other user must allow monitoring. This is because coaching the first user automatically involves hearing (monitoring) the other user. If your supervisors will be coaching calls between users, you should set up users to allow monitoring as well as coaching.

- **Personal calls can be joined**. Any user with the “Allow joining user calls” permission can add himself or herself to this user’s personal (not queue) call as a full participant.

The Security \ Permissions tab

You use the Security \ Permissions tab to define permissions and roles for the user.



For an explanation of all the user permissions, see “Wave permissions” on page 11-127.

This section describes the following:

- Before assigning permissions. See page 11-96.
- Assigning a user’s permissions. See page 11-97.
- Changing the user’s roles. See page 11-98.

Before assigning permissions

Before assigning permissions and roles to users, set up the roles (see “Managing roles” on page 11-122). A role is a template enabling you to apply the same group or collection of permissions to multiple users, so by setting up roles in advance, you can save time in giving each user the permissions he or she needs.

Assigning a user's permissions

A user's permissions determine which Wave views and features he or she can use. For an explanation of all the user permissions, see "Wave permissions" on page 11-127.

To assign the user's permissions

1 Assign the user to a role if necessary. A role is a collection of permissions. By default, new users belong to the Users role. To assign the user to a new or different role, click **Change**. See the next section for instructions.

Note: A quicker way to assign batches of users to a role is to edit the role. See "Assigning users to a role" on page 11-123.

You can assign a user to more than one role. If the roles' permissions conflict, the most permissive setting is used. For example, users who belong to both the Users role and the Administrators role have their permission for **Place external calls when logged on via a trunk** set to Allow, which is the permission level for the Administrators role.

2 If you want to give the user unique permissions, different from those of the roles to which he or she belongs, edit the user's permissions using Security \ Permissions tab. The user's **Permissions** tab settings override all role settings.

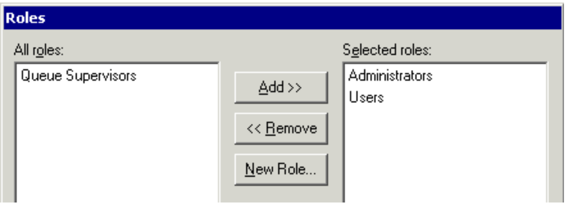
To adjust an individual permission for a user, click the **Value** column for that permission on the **Permissions** tab. Select one of the following from the drop-down list:

- **Use roles (value)**. Permission for this item is determined by the user's role memberships (described in the following section). The actual value of the permission is displayed in parentheses.
- **Allow**. The listed feature (for example, exporting Contacts) is available to the user.
- **Disallow**. The listed feature is not available to the user.
- **View and Edit**. The listed tab or folder (such as the Phone settings tab or the Call Log folder) can be viewed and edited by the user.
- **View only**. The listed tab or folder can be viewed by the user, but not edited.
- **No access**. The listed folder or tab cannot be accessed in any way by the user.

Changing the user's roles

To change the roles to which the user is assigned

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the Security \ Permissions tab.
3. Click **Change**. The Roles dialog opens.



4. Use **Add** and **Remove** to place the roles to which the user should belong in the **Selected roles** list.

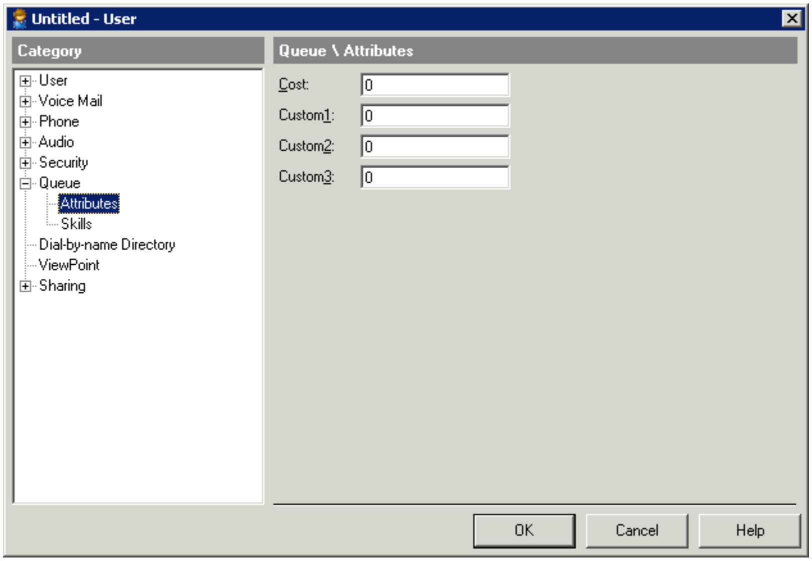
   To create a new role, click **New Role**. See "Creating a new role" on page 11-123 for instructions.

5. Click **OK**.

   Note: If the user belongs to no roles, by default the user's permissions are all set to deny access.

The Queue \ Attributes tab

If you are using the Wave Contact Center, you use this tab to assign a cost to the agent (in order to factor the cost of an agent into call distribution), or assign pre-defined custom attributes that affect call distribution to the agent.

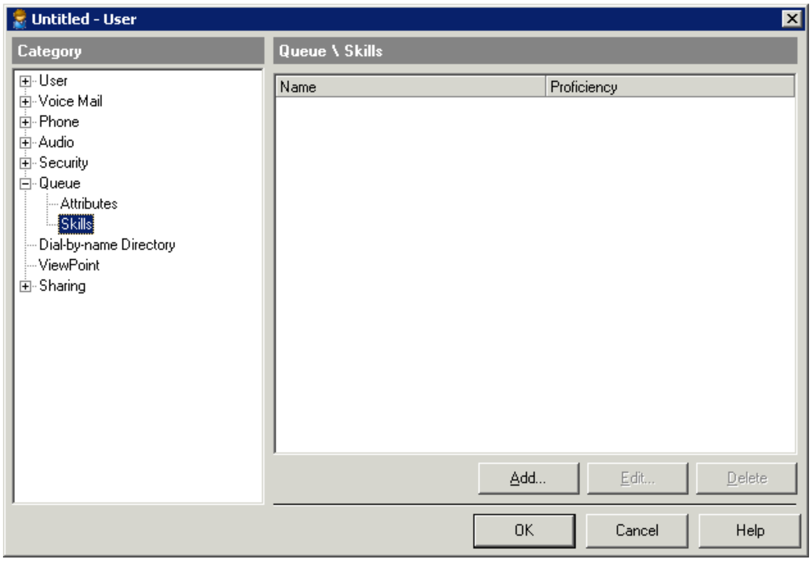


Cost: 0
Custom1: 0
Custom2: 0
Custom3: 0

For details about how to use custom call routing, see the *Wave Contact Center Administrator Guide*.

The Queue\ Skills tab

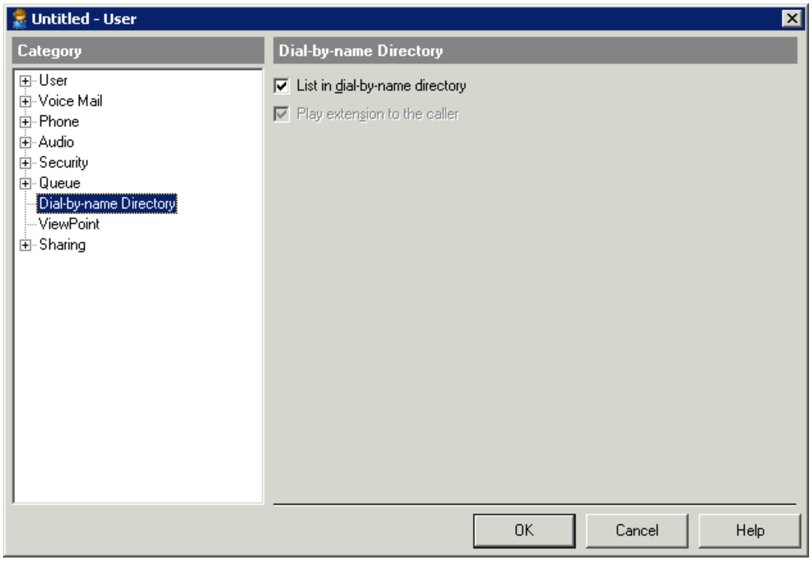
If you are using the Wave Contact Center, you use this tab to assign pre-defined skills to the user in order to route calls based on agents’ skill levels.



For details about how to use skills-based call routing, see the *Wave Contact Center Administrator Guide*.

The Dial-by-name Directory tab

You use the Dial-by-name Directory tab to specify whether the user can be looked up by name by callers who don’t know the user’s extension.



Dial-by-name Directory

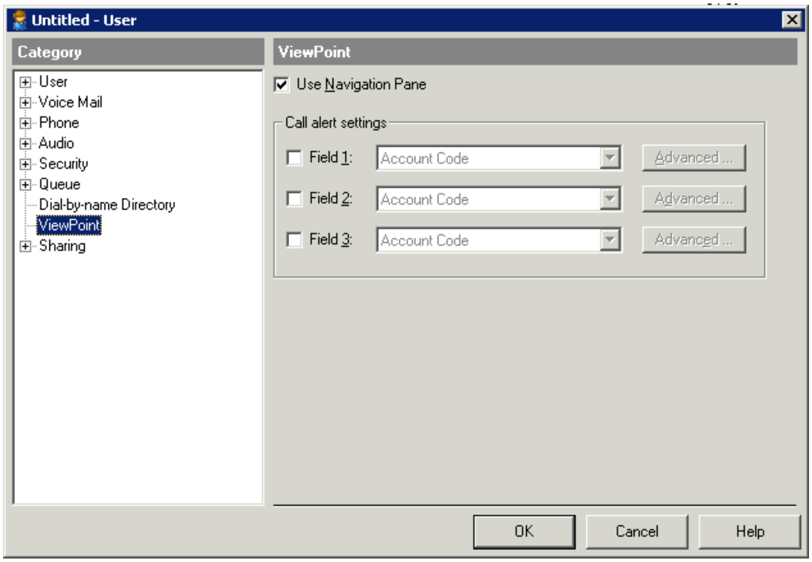
☑ List in dial-by-name directory

☑ Play extension to the caller

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the Dial-by-Name tab.
3. To include a user's name in the dial-by-name directory that callers can search, check **List in dial-by-name directory**, and make sure that the user has a voice title recorded.
4. To play a user's extension along with the user's name when callers choose the user from the dial-by-name directory, check **Play extension to the caller**.

The ViewPoint tab

Note: The **Use Navigation Pane** checkbox on this tab is not supported in this version.



Untitled - User

Category
- User
- Voice Mail
- Phone
- Audio
- Security
- Queue
- Dial-by-name Directory
- ViewPoint
- Sharing

ViewPoint

☑ Use Navigation Pane

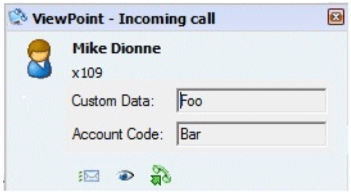
Call alert settings

□ Field 1:	Account Code	Advanced ...
□ Field 2:	Account Code	Advanced ...
□ Field 3:	Account Code	Advanced ...

You use this tab to set custom ViewPoint call alert options for the user.

When a ViewPoint user receives an incoming call, an Incoming Call Alert window pops up. By default, the Incoming Call Alert window displays only the name and phone number of the caller. You can specify up to 3 additional Call Monitor fields to be displayed in the Incoming Call Alert window. You can specify standard ViewPoint Call Monitor fields as well as custom variables that you have defined.

The following example shows an Incoming Call Alert window with the 2 default fields and 2 custom fields (Custom Data and Account Code):



ViewPoint - Incoming call

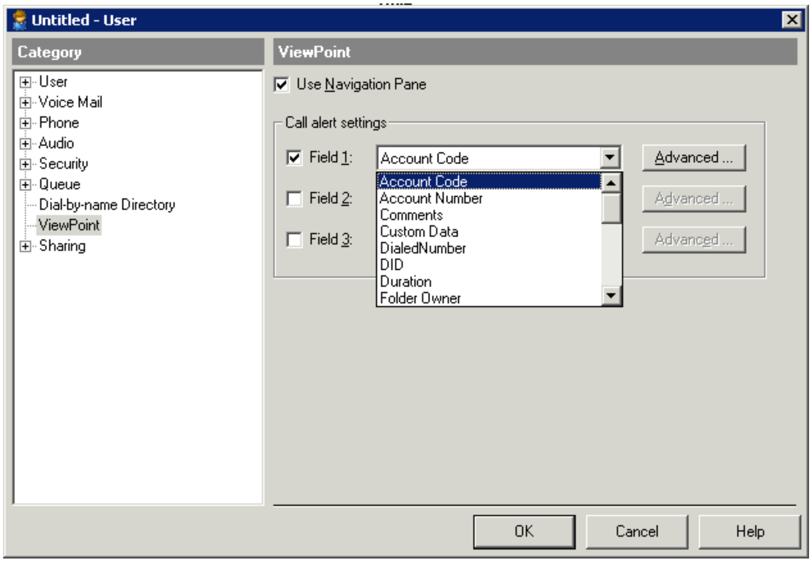
Mike Dionne
x109

Custom Data: Foo
Account Code: Bar

By default, any field that you select is displayed with its own Call Monitor label and full contents. Optionally, you can supply a custom label for the field and modify how the field's data is displayed as described below.

To set custom call alert settings for a user

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the ViewPoint tab.
3. Select the **Field 1** checkbox.
4. Select the field to display in the Incoming Call Alert window in ViewPoint from the drop-down list.



Untitled - User

Category: User, Voice Mail, Phone, Audio, Security, Queue, Dial-by-name Directory, ViewPoint, Sharing

ViewPoint

☑ Use Navigation Pane

Call alert settings

☑ Field 1: Account Code

☐ Field 2:

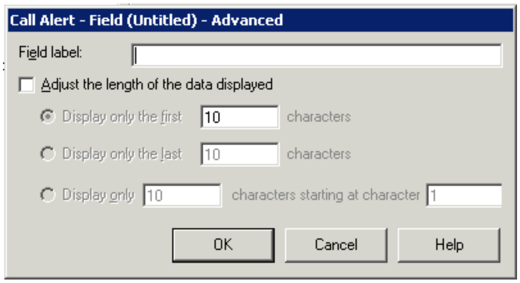
☐ Field 3:

Drop-down list: Account Code, Account Number, Comments, Custom Data, DialedNumber, DID, Duration, Folder Owner

5. Click **Advanced** to define how the specified data will be displayed for an alerting call in ViewPoint, for example to define a custom label or display only part of the data.

   Important! In this version, a size restriction on the Incoming Call Alert window in ViewPoint prevents it from displaying all data for all 3 fields. Click **Advanced** to modify the data so that the most relevant data is visible without the user having to manually resize the Incoming Call Alert window. (Note that once a user resizes the Incoming Call Alert window, the new size will be retained when the window is displayed for subsequent calls.)

The Call Alert - Advanced dialog opens:



Call Alert - Field (Untitled) - Advanced

Field label:

□ Adjust the length of the data displayed

● Display only the first 10 characters

○ Display only the last 10 characters

○ Display only 10 characters starting at character 1

6 Enter the following information:

- **Field label**. Enter a custom label for the selected field.
- **Adjust the length of the data displayed**. Select this checkbox to trim the information displayed. (If unchecked, the entire contents of the field are displayed.) Click one of the following:
    - **Display only the first ___ characters**. Enter the number of characters to display, starting with the first character.
    - **Display only the last ___ characters**. Enter the number of characters to display, starting with the last character.
    - **Display only ___ characters starting at character ___**. Enter the number of characters to display and indicate the starting character.

7 Click **OK** to save your settings.

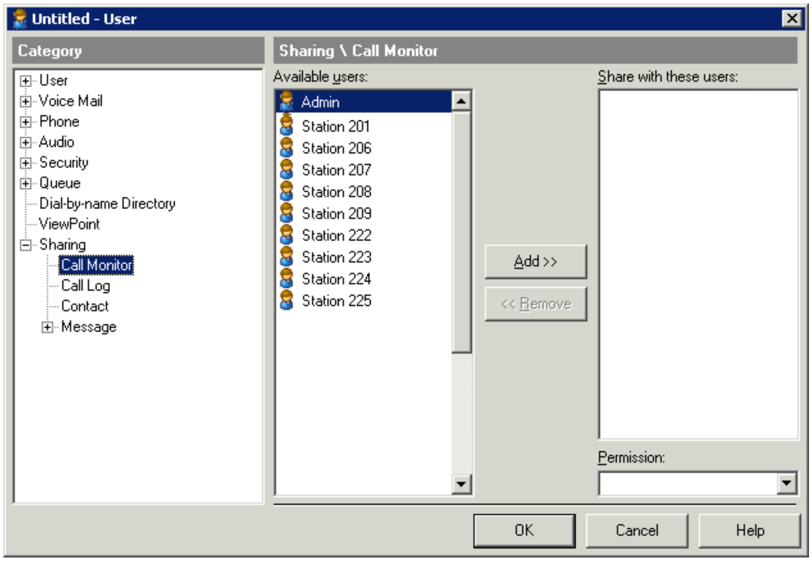
8 Repeat these steps to specify up to 3 custom alert settings for this user.

The Sharing tab

You use the Sharing tab and subtabs to share one or more of this users's ViewPoint folders with other users. For example, members of a project team may want to share contacts, call information, voice messages, and so forth.

Expand the Sharing tab in the category pane tab to select the appropriate tab to share any of the following folders:

- **Call Monitor**. Contact Center queue calls are not displayed in a shared Call Monitor.
- **Call Log**.
- **Contacts folder**.
- **Messages folder** including the Inbox, Saved, and Deleted subfolders. Voice messages marked Private do not appear in a shared folder.



The following steps describe how to share a folder via any of the Sharing tabs.

To share the user’s folder with other users

1. In the User/Group Management applet, in the Users view create a new user or double-click an existing user to edit the user.
2. Click the Sharing tab for the folder that you want to share.
3. In the **Available users** list, select one or more users with whom the folder will be shared.
4. Click **Add** to add the selected users to the **Share with these users** list.

   Click **Remove** to remove selected users from the **Share with these users** list.
5. Select one of the following access levels from the **Permission** drop-down list. The users that you select can access the folder contents based on the access level that you select.
   - **View only**. Users can view or listen to items in this folder, but cannot edit or delete them.
   - **View and Edit**. Users can view, listen to, edit, move, and delete items from this folder.

     Note: A user with View and Edit permission can delete voice messages from another user’s shared folder. If that other user has also shared his or her Deleted folder, the deleted message is moved to that Deleted folder. If that other user has not shared his or her Deleted folder, the deleted message is permanently removed.

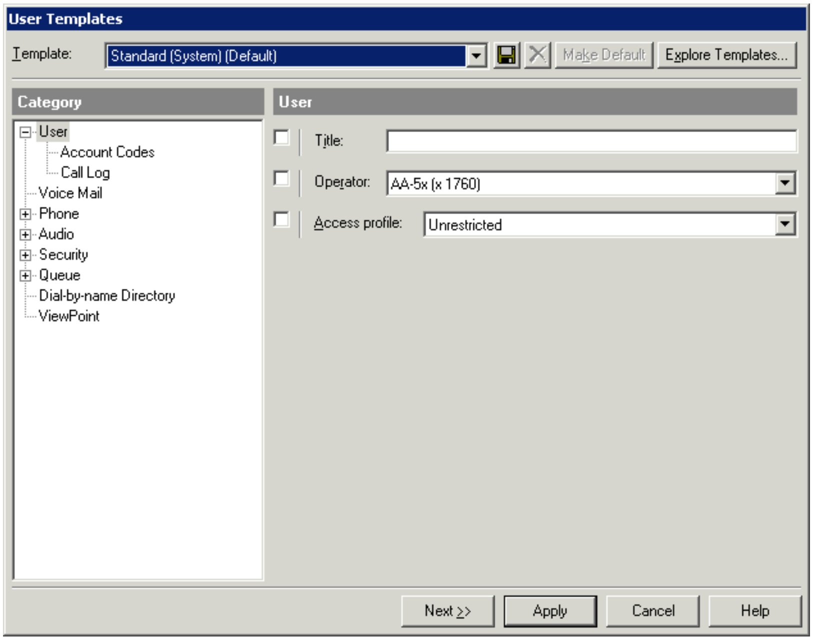
Creating and updating users via a user template

You can use user templates to do the following:.

- **Create new users quickly**. Instead of editing all of a new user's settings via the individual User dialog tabs, you can create a new user using the minimum required fields and then apply a user template (for example, "Tech Support Rep template") to fill in the rest of the settings for that type of user. If necessary, you can then go in and do any final customization required on settings not covered by the template.
- **Apply user settings in bulk**. You can quickly update the settings for multiple users by making changes in a user template that you then apply to all users associated with that template.

About the User Template dialog

To open the User Template dialog, in the User/Group Management applet choose **Tools > User Templates**.



Template: Standard (System) (Default)

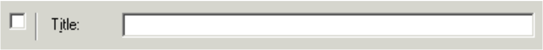
□ Title:

□ Operator: AA-5x (x 1760)

□ Access profile: Unrestricted

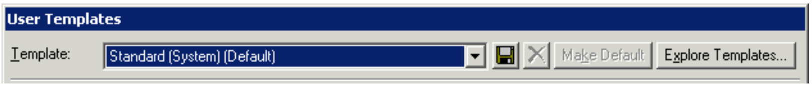
The User Templates dialog is similar to the User dialog, but there are fewer tabs and some tabs have fewer settings than the corresponding User dialog tab. See “User Templates dialog tabs” on page 11-109 for details.

Also, each user template setting is preceded by a checkbox:



If the checkbox to the left of a field is selected, the user’s corresponding setting will be updated when the template is applied. If you do not want the user setting to be changed, deselect the checkbox for that setting.

The following area is displayed at the top of each tab in the User Template dialog, and is used to select, save, create, or rename a user template, and also to make the currently-selected user template the default template used when you create new users via the User dialog.


User Templates

Template: Standard (System) (Default)

- **Template**. Select the user template to apply or edit from the drop-down list.

  Caution! When the User Template dialog opens, the **Template** drop-down list is automatically positioned at the first template in the list (in alphabetical order). Before starting to create a new template, make sure that you select the correct template (typically the Standard (System) template).

  - **Save As**. Click to save the current template definition under a different name.
  - **Delete**. Click to delete the selected user template.
  - **Make Default**. Click to make this the user template which will provide default values when you create a new user.
  - **Explore Templates**. Click to browse the user templates folder.

User Templates dialog tabs

The following table lists the tabs and settings available in the User Templates dialog. See the indicated User dialog section for details about how a tab or setting is used.

Use this tab	To specify	See page
User	Basic user information, including title, personal operator, and access profile. This tab also includes the **Access profile** field.	11-15 11-19
User \ Account Codes	Whether and under what circumstances Wave prompts the user to enter an account code for a call.	11-21
User \ Call Log	Whether the user's calls are logged, and whether the user belongs to an Organization.	11-23
Voice Mail	User's voice mailbox size and features. Note that WaveMail settings (for Microsoft Exchange synchronization) are not available in the User Template dialog.	11-28
Phone	Call waiting, Flash behavior, and other phone options. Note that the following phone type-specific settings are not available in the User Template dialog: • Enable multiple line appearances • Drop loop current when idle • Use mobile extensions to imitate a station on externally routed calls • SIP authorization settings • Disable softkeys	11-58
Phone \ Automatic Log Out	Phone login behavior on other users' phones.	11-83
Phone \ Ring Patterns	Configurable ring tones for internal and external calls.	11-78
Phone \ Softphone	If the ViewPoint integrated mobile softphone is enabled for the user.	11-81
Audio	Storage size for greeting and voice title files, and phone prompt language.	11-88

Use this tab	To specify	See page
Audio \ Hold Music	Personalized hold music source.	11-89
Security	Password expiration control, and whether the user's calls can be supervised.	11-94
Security \ Permissions	All user permissions, and the roles to which the user belongs.	11-96
Queue \ Attributes	Assign non-skill attributes (cost, custom attributes) to the user for call routing purposes.	*Wave Contact Center Administrator Guide*
Queue \ Skills	For skill-based call routing, define a set of skills that you can then assign to the user.	*Wave Contact Center Administrator Guide*
Dial-by-name Directory	Whether the user is listed in the Wave dial-by-name directory.	11-100
ViewPoint	ViewPoint application options.	11-102

Creating a new user template

Perform these steps to create a new user template, and identify the users to whom it will be applied.

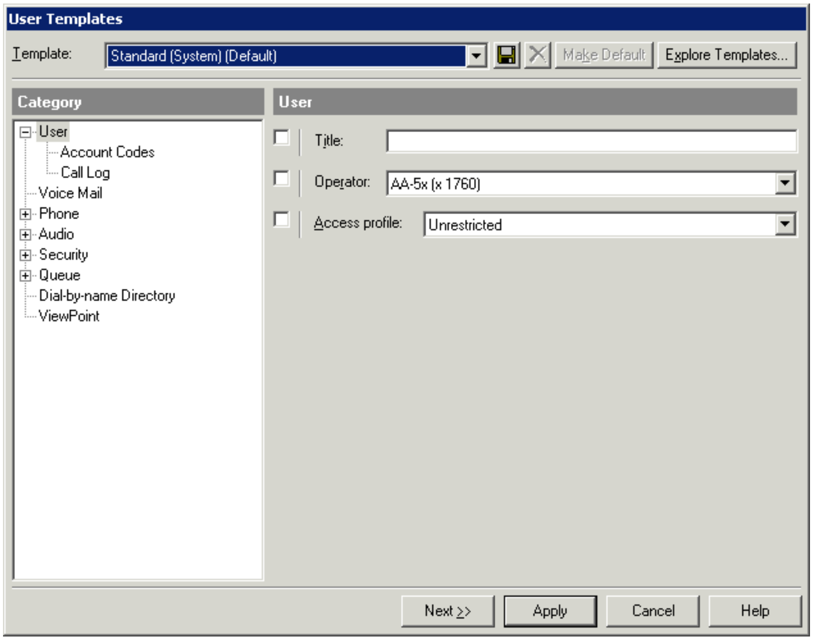
To create a new user template

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > User Templates** to open the User Templates dialog.

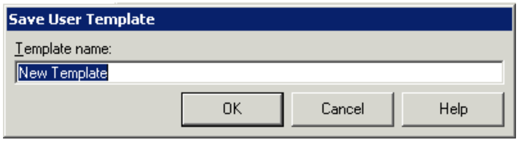


You can base your new user template on any existing template, for example “Standard (System)”.

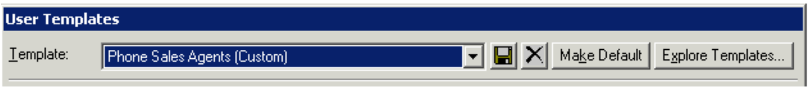
4 Select the template to start with from the **Templates** drop-down list at the top of the dialog.

5 Using the tabs in the Category pane, modify the available settings as required. See the table on page 11-109 for cross-references to sections that describe each tab and field.

6 When you are done, click 💾 at the top of the dialog to save the template under a new name. The Save Template As dialog opens:

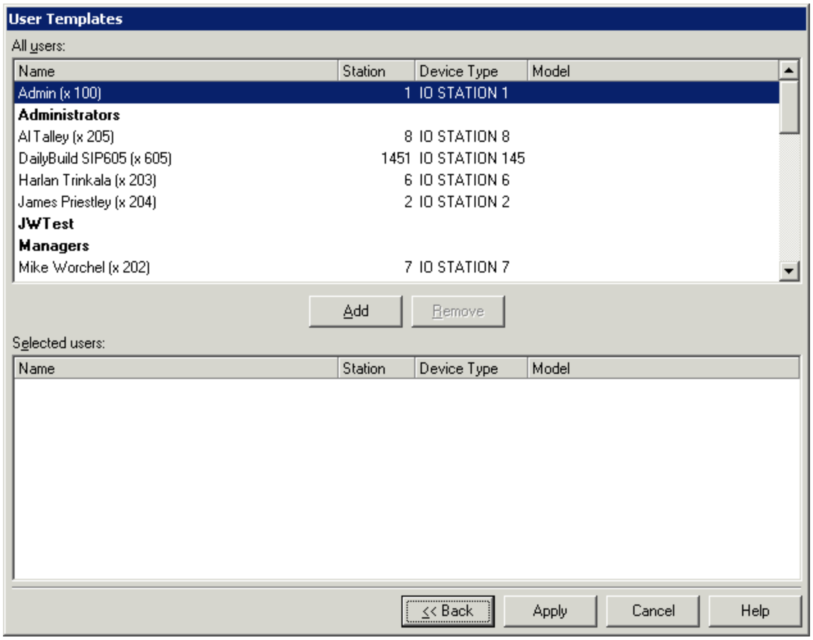


7 Enter a name for the new user template and then click **OK**. The new user template is added to the Templates drop-down list:


User Templates

Template: Phone Sales Agents (Custom)

8 Click **Next>>** at the bottom of the dialog to select one or more users and roles and apply this template to them:


User Templates

All users:

Name	Station	Device Type	Model
Admin (x 100)	1	IO STATION 1	
Administrators			
Al Talley (x 205)	8	IO STATION 8	
DailyBuild SIP605 (x 605)	1451	IO STATION 145	
Harlan Trinkala (x 203)	6	IO STATION 6	
James Priestley (x 204)	2	IO STATION 2	
JWTest			
Managers			
Mike Worchel (x 202)	7	IO STATION 7	

Selected users:

Name	Station	Device Type	Model

Click **<<Back** to return to the User Templates dialog showing all available tabs.

9 Select one or more users in the **All users** list, and then click **Add** to add them to the **Selected users** list. You can also add a group of users by selecting a Role. Roles are formatted in bold in the Users List.

10 Click **Apply** to apply the user template to the selected users.

Adding users via a user template

You specify the user template that will be used by default when you create new users via the User dialog.

To specify the default user template

1 In the User Templates dialog, select the user template in the **Templates** drop-down list.

2 Click **Make Default**.

Now, when you add a user as described in “Adding users via the User dialog” on page 11-12, the User dialog tabs will default to the values in the user template. To finish defining the user, customize the default values as needed, and define settings not included in the user template.

Applying user settings in bulk

You can use user templates to apply or change user settings for many users at once.

To apply user settings in bulk

1 Create or select a user template as described in “Creating a new user template” on page 11-110.

2 Make any changes to the template that you want to apply to the users.

3 Click **Next>>** at the bottom of the dialog.

4 Select one or more users and roles in the **All users** list, and then click **Add** to add them to the **Selected users** list.

5 Click **Apply** to apply the user template to the selected users.

Importing users via a CSV file

You can import multiple users in bulk from a comma separated values (CSV) file, rather than add users one at a time (as described in “The User tab” on page 11-15).

This section describes how to do the following:

- Prepare a CSV file for importing.
- Import users from a CSV file.
- Make changes to the contents of a CSV file before importing, and then export the changed version to a CSV file.

  Note: The **Export** button only appears after you have imported a CSV file and made changes. In this version, you cannot use the **Export** button to export a complete list of all current users directly from the User/Group Management applet.

To prepare a comma-separated values (CSV) file for importing

1. In Microsoft Excel or a text editor such as Notepad, create a new file. See “Import Users CSV file format” on page 11-116 for the required layout of this file.

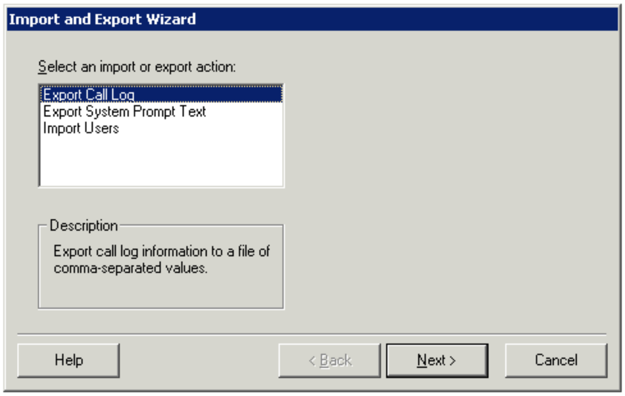
   Note: A sample user import template is available on V-Connect (choose **Products > Wave IP > Technical documents > Bulk User Import Template**).

2. Add each user to be imported as a separate row, and enter the appropriate information for each column.
3. Save the file as a CSV file to any location on the Wave Server.

To import users from a CSV file

1 In the Global Administrator Management Console, start the User/Group Management applet.

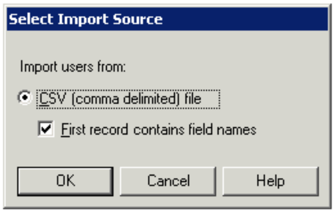
2 Click **File > Import and Export**.



Import and Export Wizard
Select an import or export action:
Export Call Log
Export System Prompt Text
Import Users
Description
Export call log information to a file of comma-separated values.
Help
< Back
Next >
Cancel

3 In the Import and Export Wizard, click **Import Users**. Click **Next** to continue.

4 In the Select Import Source dialog, select **CSV (comma delimited) file**.



Select Import Source
Import users from:
● CSV (comma delimited) file
☑ First record contains field names
OK
Cancel
Help

If your CSV file does not have a row of column headers as the first row, uncheck **First record contains field names**.

5. Click **OK**. Browse to the location of your CSV file (which must be on the Wave Server), and then click **Open**.

6. The Edit and Review Users dialog opens, where you can make final changes before importing. You can make the following changes:

   - To edit a cell, click the cell and type the new value.
   - To manually add a new user, click **New User** to create a new row in the grid, then fill in the user information.
   - To add more users from another CSV file, click **Add** to re-open the Select Import Source dialog.
   - To remove one or more users so that they are not imported, select the users and click **Remove**. Hold down the CTRL key while clicking to select multiple users.

   Optionally, click **Export** to export the list, with the changes that you've made, to a CSV file. You can save the exported file to any location on the Wave Server.

7. Click **Import**. Wave ISM will attempt to import users from the grid. If there are any users who could not be imported, the Edit and Review Users dialog reopens with errors and warnings highlighted, as follows:

   - **Errors (in red)**. Users with errors will not be imported. Errors include duplicate extensions or DID numbers.
   - **Warnings (in yellow)**. Warnings indicate users who will be imported but who may require manual intervention later to resolve ambiguities or other issues. To prevent the Edit and Review Users dialog from displaying warnings in the next pass, check **Ignore warnings**.

   Repeat step 7 until all users have been successfully imported.

Import Users CSV file format

Note the following requirements for an Import Users CSV file:

- The first row of the file can optionally contain the column headings listed in the table below. Although this is not required, it may make the file easier to work with.
- The columns of data must stay in the order indicated. Note that the fields are the same as those in the User dialog.
- If you omit a column (accepting the default value for that column for a user), you must enter a comma (,) as a placeholder for that column.

For an example that shows the contents of a CSV file containing 12 users, see page 11-119.

CSV file format for inputting users

Column	Column Heading	Contains	Comments
1	**First Name**	User's first name.	Optional. Can be left blank.
2	**Last Name**	User's last name.	Required.
3	**Extension**	User's extension.	Required. Must be unique. Numeric field can not be more than 7 digits.
4	**Slot**	Slot number assigned to user's phone.	Optional. Numeric. To create virtual extensions, leave Slot and Port blank or set to 0.
5	**Port**	Port number assigned to user's phone.	Optional. Numeric. To create virtual extensions, leave Slot and Port blank or set to 0.
6	**MAC Address**	MAC address of the user's SIP phone.	Required for SIP phone users only. 12 digit hexadecimal number unique to each user. If **MAC Address** is entered, Phone Type should be any SIP phone and Slot and Port fields should be left blank.
7	**Telephone Type**	String containing name of the phone family for the user, for example "Edge 100-12".	Required. This is the same name visible in the **Telephone Type** drop-down list on the User tab in the User/Group Management applet. Note the following: When entering a digital or IP telephone type, omit the word "Digital" or "IP". For example, enter "Edge 100-12" here, not "Digital Edge 100-12". For an analog phone user, enter "Analog".

CSV file format for inputting users

Column	Column Heading	Contains	Comments
8	**User Template Name**	Name of the user template be applied to this user.	**Optional for analog and SIP phone users.** If this field is left blank, the default user template will be applied. **Required in the current version for digital phone users.** You must supply the correct phone template name when importing digital phone users to ensure that a valid slot and port is assigned to the phone, and a Primary line feature button is defined.
9	**Phone Template Name**	Name of the phone template to be applied to the user.	Optional. This template name depends on the telephone type entered and must exist. If this field is left blank, default features will be applied to the phone.
10	**Access Profile**	Name of access profile.	Required. This must match an Access Profile name listed in the Outbound Routing applet.
11	**Title**	User’s title.	Optional.
12	**Password**	User’s password that controls access to the user's voicemail and account options. Also used to log into ViewPoint.	Optional. Numeric.
13	**Comments**	Descriptive comments about this user.	Optional.
14	**Home Phone**	User’s home phone number.	Optional.
15	**Home Phone 2**	User’s alternate home phone number.	Optional.
16	**Mobile Phone**	User’s mobile phone number.	Optional.
17	**Call Forwarding Number**	User’s call forwarding number.	Optional.

CSV file format for inputting users

Column	Column Heading	Contains	Comments
18	**E-mail**	User’s e-mail address.	Optional. Text field used for reference only—not used in system operation.
19	**E-mail 2**	User’s alternate e-mail address.	Optional. Text field used for reference only—not used in system operation.
20	**IM Address**	User’s instant messaging address.	Optional. Text field used for reference only—not used in system operation.
21	**E-mail Notification Address**	E-mail address to which voice message notifications for this user are sent.	Optional. Text field.
22	**Pager Notification Address**	Pager number to which voice message notifications for this user are sent.	Optional. Text field.
23	**Call Notification Number**	Phone number to which call notifications for this user are sent.	Optional. Text field.

In the following example of an Input Users CSV file, the first row in the file lists the column headings:

```
First Name,Last Name,Extension,Slot,Port,MAC Address,Telephone
Type,User Template Name,Phone Template Name,Access
Profile,Title,Password,Comments,Home Phone,Home Phone 2,Mobile
Phone,Call Forwarding Number,E-mail,E-mail 2,IM Address,E-mail
Notification Address,Pager Notification Number,Call Notification
Number
```

```
DANIEL,SMITH,150,,,,Comdial 8012,Basic,Unrestricted,,1150,
,,,,,,,,,,

PAUL,JOHNSON,151,,,,Comdial 8024,,Basic,Unrestricted,,1151,
,,,,,,,,,,

MARK,WILLIAMS,152,,,,Edge 100-12,,Agent,Unrestricted,,1152,
,,,,,,,,,,

ELIZABETH,ANDERSON,153,,,,Edge 100-24,,Basic,Unrestricted,,
1153,,,,,,,,,,,

JENNIFER,THOMAS,154,,,,Edge 700-24,,Basic,Unrestricted,,1154,
,,,,,,,,,,

WILLIAM,JACKSON,155,,,,Edge 700-8,,Basic,Unrestricted,,1155,
,,,,,,,,,,

DAVID,WHITE,156,,,,ImpactSCS 8312SJ,,Basic,Unrestricted,,1156,
,,,,,,,,,,

RICHARD,MARTIN,157,,,,ImpactSCS 8324SJ,,2 Lines,Unrestricted,,
1157,,,,,,,,,,,

CHARLES,THOMPSON,158,,,,Comdial 8024,,,Unrestricted,,1158,
,,,,,,,,,,

JOSEPH,GARCIA,159,,,,Vodavi 30 Executive,,Basic,Unrestricted,,
1159,,,,,,,,,,,

THOMAS,MARTINEZ,160,,,,Vodavi 8 Enhanced,,Basic,Unrestricted,,
1160,,,,,,,,,,,

PATRICIA,ROBINSON,161,,,,Vodavi 8 Executive,,Basic,
Unrestricted,,1161,,,,,,,,,,,
```

Deleting a user

Deleting a user prevents that user from using Wave and removes all of the user’s voicemail files from the system (the user's voice messages are deleted even if the mailbox is shared with another user). A deleted user’s Call Log entries are left in place to maintain an accurate and complete call history on the system.

Hint: Before deleting a user, archive their voice messages to WAV or MP3 files for later retrieval if needed.

To delete a user, in the User/Group Management applet, right-click the user and then select **Delete**.

Important! A warning is displayed if you try to delete a user who is currently being used as a target location of any kind, for example:

> “This user is currently being used as a routing list target: [Name] (extension). Edit or delete these locations before deleting this user.”

The warning is displayed if you try to delete a user who is currently being used as any of the following, and contains the indicated information:

- Forward-to extension: [Name] (extension)
- Intercept destination: [Name] (Trunk Group)
- Also ring extension: [Name] (Trunk Group)
- Call notification: [Name] (extension, Cascading Notification Rule: [Rule Name])
- Call notification: [Name] (extension)
- Routing List target: [Name] (extension)
- Menu choice for auto attendant: [AA Name] extension)
- ViewPoint Group member: [Group Name]
- Operator: [Name] (extension)

Managing roles

Roles are groups that enable you to apply the same set of permissions to multiple users. You can create as many different roles as you want, to represent different groups of users who have similar permissions. Roles appear in the Users view in bold.

When a user belongs to a role, he or she inherits the role's permissions. A user can belong to more than one role, in which case the most permissive settings apply in cases of conflict.

You can grant a user individual permission settings that override those of the role, by adjusting his or her permissions individually on the Permissions tab of the User dialog. See "The Security \ Permissions tab" on page 11-96.

Wave comes with the following three roles:

- **Administrators**. You cannot delete this role, but you can edit some of its settings. By default the role has full permissions. You can disallow only the following permissions:
  - Log on via a station
  - Log on via a trunk
  - Log on via a SIP trunk
  - Place external calls when logged on via a trunk
  - Place external calls from a station
  - Forward or route calls to external numbers
  - Return calls when logged on via a trunk

  The Admin user belongs to the Administrators role by default.
- **Users**. By default new users belong to this role.
- **Managers**. The Managers role should be used for end-user managers who need access to some system settings, but not full administrative access. This role's permissions can be fully customized.

Assigning users to a role

The quickest way to assign a batch of users to a role is to edit the role and add the users. See “Creating a new role” on page 11-123.

You can also assign a user to a role by editing the user. See “The Security tab” on page 11-94.

Editing a role

To edit an existing role, double-click it in the Users view. For further instructions, see the next section.

When editing a role, be aware of the following:

- When you change a role’s permissions, those permissions change for all users belonging to the role, except where a user’s individual permission setting overrides the role, or where a user’s other role provides a more permissive setting.
- When you remove a user from a role, the user loses all permissions granted by that role.
- The Administrators role can only be edited in limited ways.

Creating a new role

You can create a new role, for example Admin Assistant, for a group of users that require the same or similar permissions. All users that you assign to this role are automatically granted its permissions, except where their individual permission settings override the role settings.

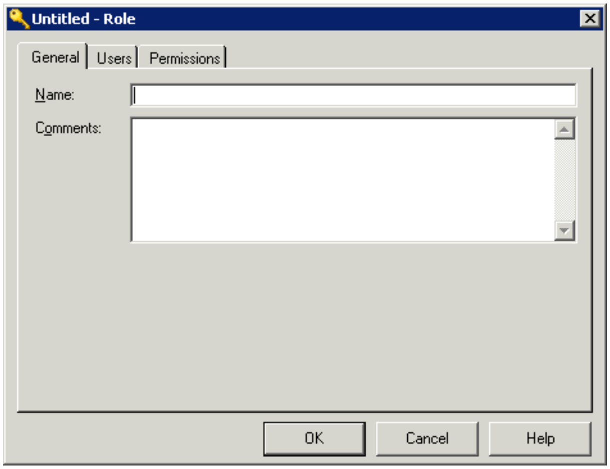
To create a new role

1 If necessary, click the Administration tab of the Management Console.

Click

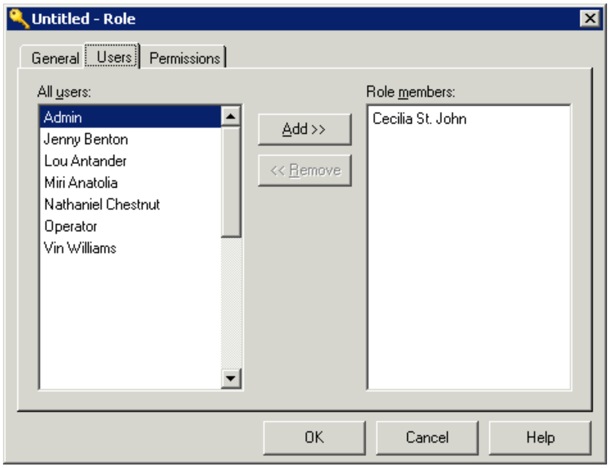
2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

1 Choose **File > New > Role**. The Role dialog opens.



2 Enter a short, descriptive **Name** for the role (for example, “Sales”) and any **Comments** about how it will be used.

3 Click the Users tab to identify which users belong to the role.

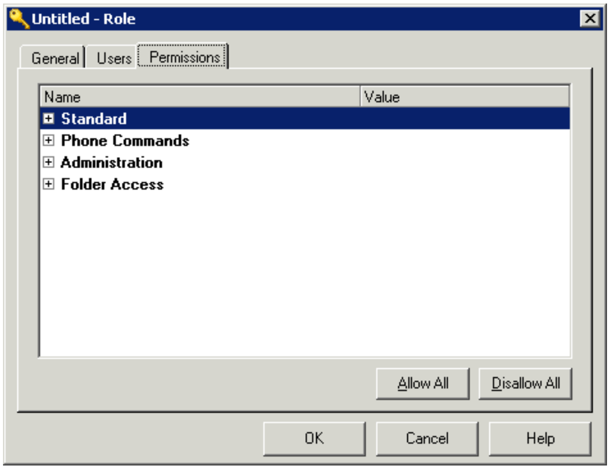


All users:
Admin
Jenny Benton
Lou Antander
Miri Anatolia
Nathaniel Chestnut
Operator
Vin Williams

Role members:
Cecilia St. John

- To add users to the role, select them in the **All users** list and click **Add**.
- To remove a user from the role, select the user in the **Role members** list and click **Remove**.
- To select several users at once, hold down SHIFT or CTRL as you click.

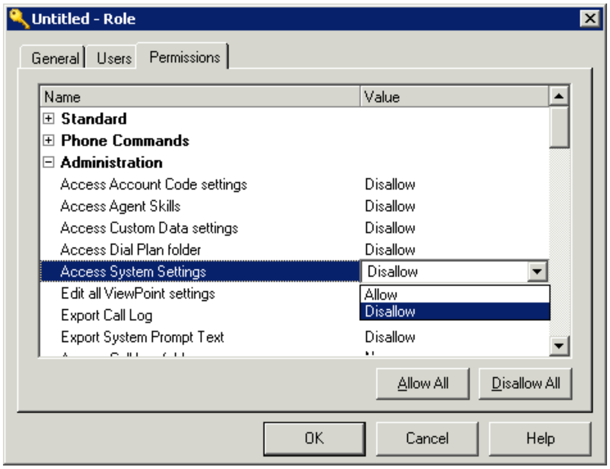
4 Click the Permissions tab to define the features and folders that members of a role can or cannot access.



Name	Value
⊞ **Standard**	
⊞ **Phone Commands**	
⊞ **Administration**	
⊞ **Folder Access**	

For a description of each category and the permissions in that category, see “Wave permissions” on page 11-127.

5 To set a permission, expand a category and click on the permission, and then select the permission level from the **Value** drop-down list.



Name	Value
⊞ **Standard**	
⊞ **Phone Commands**	
⊟ **Administration**	
Access Account Code settings	Disallow
Access Agent Skills	Disallow
Access Custom Data settings	Disallow
Access Dial Plan folder	Disallow
Access System Settings	Disallow
Edit all ViewPoint settings	
Export Call Log	
Export System Prompt Text	Disallow

Depending on the permission, you can specify a value from either of the following groups:

- **Allow** / **Disallow**. The selected feature or item is or is not available to the role member.
- **View and Edit** / **View Only** / **No access**. The listed tab or folder:
  - Can be viewed and edited by the role member
  - Can be viewed by the role member, but not edited.
  - Cannot be accessed in any way by the role member.

6 You can also set permissions by clicking the following buttons:

- **Allow all**. Sets all permissions to “Allow” or “View and Edit” for this role.
- **Disallow all**. Sets all permissions to “Disallow” or “No access” for this role.

Important! The Administrators role is handled differently than other roles—the only permissions that are changed by clicking **Allow all** or **Disallow all** are the ones related to dialing, to help control toll fraud. See “Disallowing security-risk user permissions” on page A-5 for a list.

7 Click **OK** to close the Role dialog.

Wave permissions

A user's access to Wave features is controlled by permissions. There are two types of Wave permissions:

- **General user permissions**. These control what ViewPoint views and Wave commands the user can use. See the next section.
- **Contact Center agent permissions**. These apply only to agents in a Contact Center queue, and control what queue features the agent can use. For details, see Chapter 2 in the *Wave Contact Center Administrator Guide*.

Users inherit general permissions and dialing permissions from the *roles* to which they belong. (A role is a collections of permissions that you set up to define a job or role in your organization.) See "Managing roles" on page 11-122. Users can also have individual permissions that override the permissions of the roles to which they belong.

Wave permission changes made via the User/Group Management applet are not reflected in ViewPoint until after the affected user restarts ViewPoint.

General user permissions

You can assign permissions in any of the following ways:

- To assign permissions to a role, see "Creating a new role" on page 11-123.
- To assign individual permissions to a user, see "The Security tab" on page 11-94.
- To assign permissions via a user template, see "Creating a new user template" on page 11-110.

The following table describes the permissions that you can define for individual users or roles.

Wave General User Permissions	
Permission	**Controls the ability to...**
Standard user permissions These permissions control the ability to use specific Wave Server features.	
Access Call Center Reporter	Controls the ability to use the Contact Center Reporter to run reports from ViewPoint. For more about running ViewPoint reports, see Chapter 13 in the *Wave ViewPoint User Guide*.

Wave General User Permissions	
Permission	**Controls the ability to...**
Add parties when replying to voicemail	Controls the ability to send voicemail replies to additional users as well as the sender. (Applies only to replying to voice messages via ViewPoint.)
Allow coaching/joining/ monitoring user calls	Controls the ability to coach, join, or monitor other users' calls. Note that the target user must also be set up to permit call supervising (see "Configuring whether the user's calls can be supervised" on page 11-95).
Allow ViewPoint Mobile Connection	Controls the ability to use the Mobile ViewPoint Client to make and take calls and access some ViewPoint features from supported mobile devices, such as an iPhone, iPad and so forth.
Place external calls when logged on via a trunk	Controls the ability to dial in to Wave from a remote location and place external calls through the Wave Server that get billed to that Wave Server.
Place external calls from a station	Controls the ability to place outbound calls on Wave trunks.
Change Personal Status	Controls a user's ability to change his or her own personal status. Note that in a Contact Center environment, disallowing this permission for agents helps ensure that they take calls during their shifts.
Change the Personal Status of any user	Controls a user's ability to change their own or another user's personal status using the **Apply Personal Status** command in ViewPoint. Note that the user must enter the other user's password to change that user's personal status.
ViewPoint call control	Controls a user's ability to use the ViewPoint Call Monitor to handle calls.
Delete Call Log entries	Controls a user's ability to use the **Edit > Delete** command in the Call Log in ViewPoint or in the User/Group Management applet.
Export data	Controls a user's ability to export contacts, extensions, or the Call Log via ViewPoint.
Forward or route calls to external numbers	Controls a user's ability to specify an external number when forwarding calls or setting up routing lists.
Forward voicemail	Controls a user's ability to controls a user's ability to forward voice messages to one or more users.
Allow Instant Messaging	Controls the ability to send and receive instant messages in ViewPoint.
Allow inter-organizational Instant Messaging	Controls the ability to send and receive instant messages with users in Wave organizations other than the one the user belongs to. The **Allow Instant Messaging** permission must be enabled in order for a user to send and receive inter-organizational instant messages.

Wave General User Permissions	
Permission	**Controls the ability to...**
Log on via IP trunk	Controls a user’s ability to log on while on a SIP call to Wave.
Log on via station	Controls a user’s ability to log on by pressing **#** at a Wave phone.
Log on via trunk	Controls a user’s ability to log on when calling from a remote location, either via the auto attendant or by pressing **9** at a voicemail greeting.
Change password	Controls a user’s ability to change his or her own Wave password.
Off-hook page	*This permission is not currently implemented.*
Pick up other ringing call	*This permission is not currently implemented.*
Play audio into a call	*This permission is not currently implemented.*
Record calls	Controls a user’s ability to record calls using the Call Monitor. **Important:** It is the license-holder’s responsibility to comply with any federal, state, or other applicable statutes regarding the recording of phone calls. Vertical Communications, Inc. disclaims any responsibility for failing to comply with such regulations. Some countries, states, or other locations require that you announce to callers that their calls may be or are being recorded. Be sure to instruct any users with this permission (or who inherit this permission from a role) how to comply with call recording privacy requirements. For more information, see “Privacy issues with call recording” on page 19-2.
Reply to voicemail	Controls a user’s ability to send a voice message as a reply to a received voice message.
Report on all Call Logs	Controls a user’s ability to run the Call Log report on the Call Log of any user or queue. When set to **Disallow** (the default), the report can be run only on the Call Log of the user logged in to the Reporter in ViewPoint. For more about the Call Log report, see Chapter 13 in the *Wave ViewPoint User Guide*.
Return external calls when logged on via a trunk	Controls the ability to use the **43** or **44** commands to call back a voice message from an external number, when calling in from a remote location.
Show ‘All’ tab in ViewPoint Extensions view	Controls the ability to see the “All” tab in ViewPoint’s Extensions view, which shows all extensions in the system. (With this tab turned off, the user can still see the filtered tabs, such as tabs for ViewPoint Group or call center queue extensions.)
Synchronize voice mail and contacts	Controls the ability to use Wave Mail to synchronize a user’s voice messages and contacts between Wave and the user’s e-mail program.

Wave General User Permissions	
Permission	**Controls the ability to...**
Access... settings	Controls the ability to view and use the specified feature, available in ViewPoint's Options dialog (**Tools > Options**). You can set individual permissions for the following settings: • Call notification settings • Dial by name settings • E-mail notification settings • Message settings • Operator setting • Pager notification settings • All phone behavior settings • Prompt language setting • All call screening settings
Access voice title	Controls the user's ability to record his or her own voice title, using ViewPoint, the User/Group Management applet, or the phone commands. (This permission does not affect the ability to record or capture voice titles for contacts.)
Phone Commands permissions These permissions control the ability to enter specific feature commands via the phone.	
Access saved messages	Controls the ability to press **2** after logging on to access voice messages in the Saved folder.
Callback last incoming call	Controls the ability to dial ***69** to return the most recent incoming call.
Dial by name	*This permission is not currently implemented.*
Manage account settings	Controls the ability to use the **6** command from the Voicemail / Account menu to manage account preferences.
Send message to all	Controls the ability to send a voice message to 8888#, which sends the message to all users.

Wave General User Permissions	
Permission	**Controls the ability to...**
Set personal status:	Controls the ability to set the specified personal status by logging in and pressing **6 1 x**. You can set individual permissions for the following personal statuses: • Available (Non-Queue) • Available • Available (Queue Only) • Do Not Disturb • In a Meeting • On Break • On Vacation • Out of the Office The permissions for Available (Non-Queue), Available, and Available (Queue Only) control the ability to dial ***50-*52** to set that personal status.
Start a new call via #	Controls the ability to press **#** for dial tone to dial a new call from either the Voicemail / Account menu (after logging on) or the Call Handling menu (after pressing Flash).
Administration permissions These permissions control the ability to perform specific administrative functions:	
Access...	Controls the ability to view and be able to use the specified feature in the User/Group Management applet. You can set individual access permissions for the following features: • Account Code settings • Agent Skills • Custom Data settings • Dial Plan folder • System Settings
Edit all ViewPoint settings	Controls the ability of the specified user to log on to ViewPoint (using a command line switch) and edit another user’s ViewPoint settings without knowing the user’s ViewPoint password. This is a global permission that gives this user access to all other users on the system. See *“Modifying a user’s ViewPoint settings” on page 11-133*.
Export Call Log	Controls the ability to export the Call Log via the User/Group Management applet.
Export System Prompt text	Controls the ability to export system prompts to a text file via the User/Group Management applet.

Wave General User Permissions	
Permission	**Controls the ability to...**
Access... folder	These permissions control the degree of access the user has to the specified folder in the User/Group Management applet. The choices are: **No access**. The folder view does not appear in the User/Group Management applet. **View only**. The user can view but not edit or delete the folder's items. **View and Edit**. The user has full access to the folder. You can set individual access permissions for the following folders: • Call Log folder • Auto Attendants folder • Dialing Services folder • Public Contacts folder • Public Workgroups folder • IVR Plug-ins folder • Maintenance Log folder • Pickup Groups folder • Queues folder • System Prompts folder • Users folder Note that the permission "Access Queues folder" enables a user to sign agents in and out of any queue, including themselves if they are non-observer agents. This permission overrides the per-queue permission "Queue sign in/out", set via the Queue dialog. For more information about setting queue permissions, see Chapter 2 in the *Wave Contact Center Administrator Guide*. Note that the objects shown in the Dial Plan view are edited using the permissions for other folders (Users, Queues, etc.), so the permission "Access Dial Plan" folder has an Allow/Disallow choice.

Wave General User Permissions	
Permission	**Controls the ability to...**
Folder Access These permissions control whether a user has full, read-only, or no access to a particular folder view in ViewPoint. The choices are:	
Access... folder	These permissions control the degree of access the user has to the specified folder in ViewPoint. The choices are: **No access**. The folder view does not appear in ViewPoint. **View only**. The user can view but not edit or delete the folder's items. **View and Edit**. The user has full access to the folder. You can set the following individual folder view access permissions: • Call Rules folder • Contacts folder • Routing Lists folder • Workgroups folder Note that a "No access" setting prevents the user from accessing the folder even using the ViewPoint API. Disallowing a folder using the "Folder Visibility" permission removes it from ViewPoint, but still permits access via the API.

Modifying a user's ViewPoint settings

There are times when you may need to troubleshoot aspects of a user's account that can only be accessed via ViewPoint, for example to listen to and re-record the user's voicemail greetings.

Wave lets you modify a user's ViewPoint settings by logging on to ViewPoint using special command-line switches. You do not need to know the user's password, and you will have full access to all features as if you were logged in as that user. (Using ViewPoint command-line switches is described in detail in Appendix B in the *Wave ViewPoint User Guide*.)

Requirements:

- You must have ViewPoint installed to use this modify a user's ViewPoint settings.
- The user must have the Wave permission **Edit all ViewPoint settings** set.

To modify a user’s ViewPoint settings

1 Right-click the ViewPoint shortcut icon on your Windows Desktop and then choose **Properties**.

2 On the Shortcut tab, enter the following command in the **Target** text box:

Syntax:

```
“C:\Program Files\Vertical
Wave\ViewPoint\Vertical.Wave.ViewPoint.exe”
/adminuser:<adminusername> /adminpassword:<adminpassword>
/loginuser:<username>
```

- For <*adminuser*> and <*adminpassword*>, enter your Wave user account logon credentials—this must be an account with the Edit All ViewPoint Settings permission.
- For <*username*>, enter the name that the user provides when logging on to ViewPoint.

Note: Both account names should be inside quotation marks, because the normal format used for Wave user account names includes a space.

Examples:

- In this example, the administrator Jeff Bohn and user Neil Pratt are both Wave users and Jeff Bohn has the Edit All Viewpoint Settings permission:

```
/adminuser:”Jeff Bohn” /adminpassword:12345
/loginuser:”Neil Pratt”
```

3 Click **OK** to continue. ViewPoint opens with the selected user logged in. To modify many ViewPoint settings, choose **Tools > Options**. See “About customizing ViewPoint” in Chapter 12 in the *Wave ViewPoint User Guide* for details.

Chapter 12

Managing ViewPoint Groups

CHAPTER CONTENTS

A ViewPoint Group is a group of related extensions or contacts. With ViewPoint Groups you can do the following:

- Direct calls to a group of users using routing lists. The routing list can ring the Viewpoint Group using several different routing algorithms. For more about creating and using routing lists, see Chapter 9 in the *Wave ViewPoint User Guide*.

  Note: For a different method to call a group of users, use station hunt groups. See “Creating a station hunt group” on page 10-48.

- Organize groups of extensions for display in ViewPoint’s Extensions view, making it easier for users to locate an extension for calling or transferring calls.
- Create Voice Mail Distribution Group to send voice messages to multiple users simultaneously.

See the *Wave ViewPoint User Guide* for instructions on placing calls, routing calls to ViewPoint Groups, and using the Extensions view.

About public and personal ViewPoint Groups

Wave provides two types of ViewPoint Groups: public and personal.

- **Public ViewPoint Groups** are visible to all Wave users. Administrators and users with the appropriate permissions can create public ViewPoint Groups. Public ViewPoint Groups are managed in the User/Group Management applet.
- **Personal ViewPoint Groups** are created by users to easily locate a group of related extensions in the individual user's ViewPoint Extensions list. A personal ViewPoint Group is visible only to the user who created it and cannot have an extension for sending voicemail to the Group. Personal ViewPoint Groups are managed in ViewPoint (see the *Wave ViewPoint User Guide*).

About Voice Mail Distribution Groups

You can use a Voice Mail Distribution Group to send voice messages to multiple users simultaneously. You can send a voice message to a Voice Mail Distribution Group via ViewPoint or using the phone.

To send a voice message to a Voice Mail Distribution Group, do either of the following:

- In ViewPoint, choose **File > New > Voice Message**. In the New Message dialog, add the Voice Mail Distribution Group to the **Recipients** list. For more about sending a voice message directly to voice mail, see Chapter 7 in the *Wave ViewPoint User Guide*.
- Using the phone, logon and then press **3** to send a message. After recording your message and pressing **#** to finish, press **8#** and then enter the **group number** as the destination when you are prompted for an extension.

Note: You assign a group number—not an extension—when you create a Voice Mail Distribution Group. A Voice Mail Distribution Group does not have an extension and cannot be dialed directly.

Benefits of using ViewPoint Groups

ViewPoint Groups offer the following benefits:

- The process of finding an individual to take calls or to join a conference call is easier, because the Extensions view in ViewPoint can be filtered by ViewPoint Group.
- Auto attendants, queues, contacts, or IVR Plug-ins can be added to a ViewPoint Group (for informational purposes) and viewed in the Extensions view.
- Contacts can be added to ViewPoint Groups for caller identification via call rules (see the *Wave ViewPoint User Guide*).
- Viewpoint Groups can be used in routing lists to ring multiple users using different algorithms. IVR Plug-ins, auto attendants, queues, and contacts who are members of that Group are never called when a routing list rings a Viewpoint Group. Both public and a user's own private Viewpoint Groups can be used in routing lists.
- When ViewPoint Group members set their personal statuses to Do Not Disturb (see the *Wave ViewPoint User Guide* for details) their phones do not ring when the Group is called.
- When ViewPoint Group members forward their calls internally (see the *Wave ViewPoint User Guide*), calls to the Group ring at the number to which calls are being forwarded.

The ViewPoint Groups view

Use the ViewPoint Groups view in the User/Group Management applet to add, edit, and delete public ViewPoint Groups. To open it, do the following:

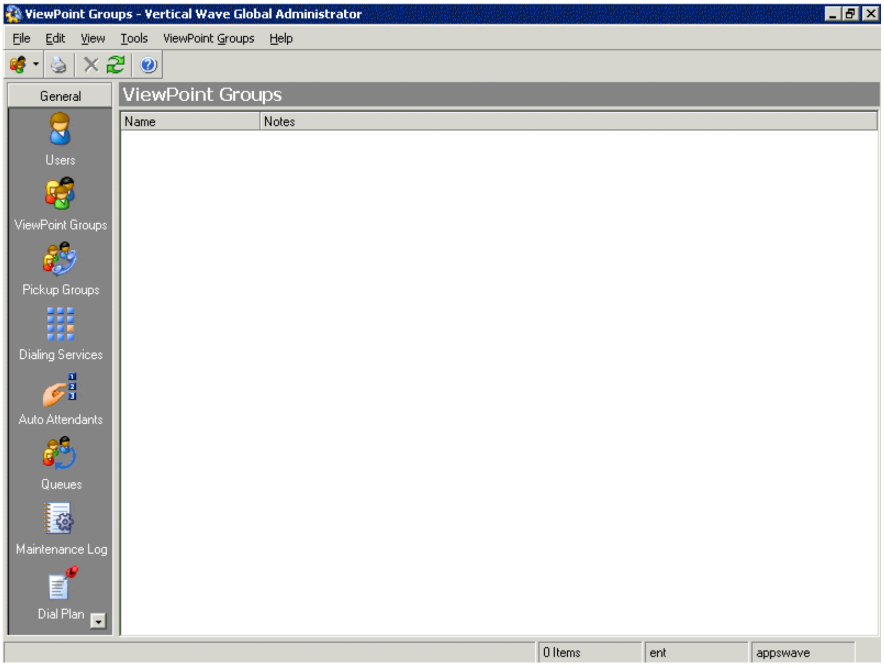
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Log on to the User/Group Management applet, which opens in a remote access window. See “Accessing the User/Group Management applet” on page 2-15 for more about logging on to the User/Group Management applet.

4 Click **ViewPoint Groups** in the view bar to open the ViewPoint Groups view.



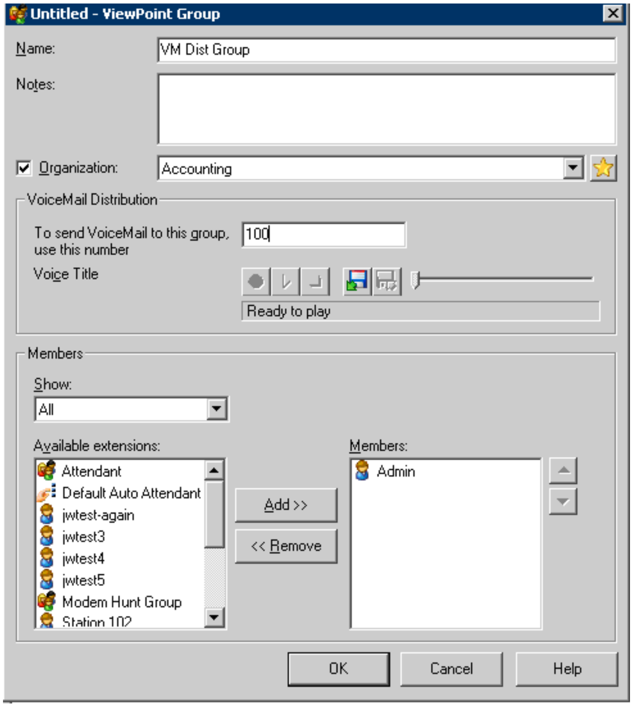
Creating a ViewPoint Group

To create a public ViewPoint Group

1 In ViewPoint, choose **File > New > ViewPoint Group** and enter information on the tabs in the Group dialog, as follows:

2 On the General tab, enter the **Name** of the ViewPoint Group and at least one member. You can optionally add a note about the Group in the **Notes** field.

3 To add members to the ViewPoint Group, select names from the list of **Available extensions** and click **Add**. To select multiple names, hold down CTRL while clicking.



Untitled - ViewPoint Group

Name: VM Dist Group

Notes:

☑ Organization: Accounting

VoiceMail Distribution

To send VoiceMail to this group, use this number: 100

Voice Title

Ready to play

Members

Show: All

Available extensions:

- Attendant
- Default Auto Attendant
- jwtest-again
- jwtest3
- jwtest4
- jwtest5
- Modem Hunt Group
- Station 102

Members:

- Admin

4 Use the arrows next to the **Members** list to arrange the order of the members. The order in which the names appear can be used in conjunction with a user who has a routing list that calls the members of this ViewPoint Group in a “top down” or “round robin” sequence (for more information about routing lists, see the *Wave ViewPoint User Guide*). You can also use the **Remove** button to delete members from the list.

5 If you are creating a Voice Mail Distribution Group, optionally complete the following fields:

- Enter a group number (1-9999) that will be used to route voice messages to the new Group. Since this number is not an extension, you do not have to worry about any extension conflicts. Enter a unique number for each Voice Mail Distribution Group.

  Note: A group number is required to send a voice message to the Group via the phone. You do not need to specify a group number when you send a voice message to the Group via ViewPoint.

- Optionally, record a **Voice Title** for the new Group using the audio controls. (See “Using the audio controls” on page 2-21.)

  When a user specifies a Voice Mail Distribution Group via the phone (as described in “About Voice Mail Distribution Groups” on page 12-2), the confirmatory prompt, “This message will be sent to the ___ group” is played, where “___” will be replaced with the title that you record here.

6 Click **OK** to save the Group.

Chapter 13

Configuring Auto Attendants

Chapter Contents

You can configure an auto attendant if you want to have the inbound calls on your company’s main phone number answered automatically. The auto attendant usually consists of a recorded greeting followed by a menu of choices. For example, your main auto attendant might say: “Welcome to Barchetta Industries. You may dial an extension at any time. For Sales, press 1. For Customer Support, press 2. To hear a recorded message about our special offers, press 3. To speak to the Operator, please hold.”

You can set up an auto attendant to let callers do any of the following:

- Dial an extension
- Dial a user by name in the dial-by-name directory
- Log in using a Wave extension and password

- Hear a recorded message
- Transfer to a user, Contact Center queue, ViewPoint Group, or IVR Plug-in
- Transfer directly to a voice mailbox to leave a message
- Transfer to another menu (another auto attendant)

You can also specify an automatic action to take if callers do nothing.

Note: You can use the **separately-licensed Wave Call Classifier add-on** to create business rules and associate those rules with an auto attendant to identify callers, intelligently route calls, and present Contact Center agents with scripts and related caller information before calls are answered. For details about using the Call Classifier add-on, see Chapter 26.

The Default Auto Attendant

When Wave is installed, you must assign all trunk groups associated with trunks to the default auto attendant at extension 560. Whenever you add a trunk group, you must also assign it to an auto attendant. You can change assignments at any time

The Default Auto Attendant plays a greeting and offers the caller the following options:

- Dial any Wave extension.
- Press **9** to access a dial-by-name directory.
- Press **0** to transfer to the Operator.
- Press **#** to log in to Wave.

Note: If three seconds pass after the greeting has played without the caller pressing any key, the call is transferred to the Operator.

Configuring an auto attendant

Configuring an auto attendant consists of the following procedures:

- “Creating a new auto attendant” on page 13-3
- “Defining menu choices” on page 13-6
- “Customizing login behavior from auto attendants” on page 13-13
- “Scheduling transfers and greetings” on page 13-16
- “Setting up an auto attendant’s hold music and greetings” on page 13-20
- “Setting up custom data and skill requirements for an auto attendant” on page 13-22

Creating a new auto attendant

To create an auto attendant

1 If necessary, click the Administration tab of the Management Console.

Click

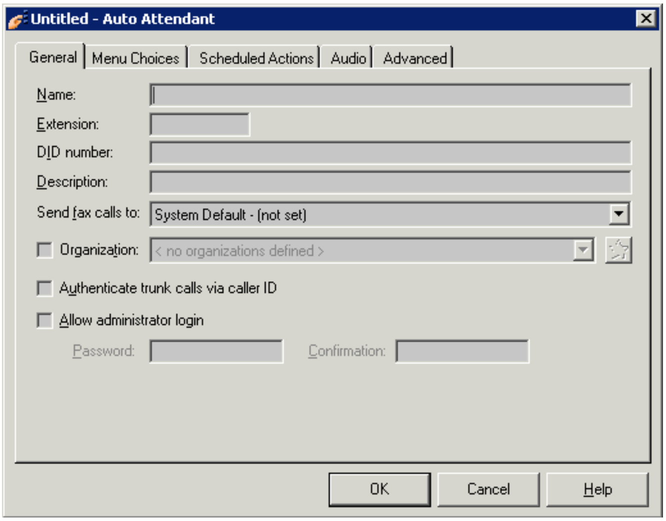
2 Click the **User/Group Management** icon, located in the PBX Administration section of the Management Console.

3 Log on to the User/Group Management applet, which opens in a remote access window. See “Accessing the User/Group Management applet” on page 2-15 for more about logging on to the User/Group Management applet.

4 Click the **Auto Attendants** icon in the view bar. The Auto Attendants view opens, showing all auto attendants that have been created so far.

The Default auto attendant is automatically provided with Wave.

5 Choose **File > New > Auto Attendant**. The Auto Attendant dialog opens.



Name:

Extension:

DID number:

Description:

Send fax calls to: System Default - (not set)

□ Organization: < no organizations defined >

□ Authenticate trunk calls via caller ID

□ Allow administrator login

Password: Confirmation:

6 Enter the following information on the General tab:

- **Name**. Required. Descriptive name for the new auto attendant, for example, “Sales auto attendant”.
- **Extension**. Required. Extension used to access the auto attendant. Wave users can transfer callers to the auto attendant at this extension. To test the auto attendant, call this extension. (The default auto attendant is assigned the extension 560.)

  Note: Extension 8888 is reserved and cannot be assigned to an individual user. Extension 8888 is reserved for the “send message to all users” feature. If a user enters extension 8888 when sending a voice message from his or her phone, the message is automatically sent to all users who have a voice mailbox configured.
- **DID number**. *This feature is not supported in this version.*
- **Description**. Information that describes the auto attendant.

- **Send fax calls to**. Select the extension to which incoming faxes to this auto attendant will be automatically redirected. Select “System Default” from the drop-down list to use the system default for fax redirection as specified via the PBX tab of the General Settings applet. For information on setting the system fax redirect default extension, see “Configuring Fax Redirect” on page 16-15.

  Note: In the drop-down list, “System Default (not set)” means that no system fax redirect default extension has been specified.

- **Organization**. Select this checkbox and select an Organization to have calls to this auto attendant logged with that Organization. Calls must end at the auto attendant to be logged with the selected Organization. If the call proceeds to a user, it will be logged with the user’s Organization. For information about Organizations, see “Using Organizations” on page 20-2.
- **Authenticate trunk calls via caller ID**. Select this checkbox to enable this auto attendant to automatically log in a user who calls from an authenticated number.
  - If this checkbox is selected, whenever a user calls this auto attendant from an authenticated number, he or she is automatically logged in without being prompted to enter an extension or password.
  - If this checkbox is not selected, a user will be prompted to enter an extension or password to log in, even if calling from an authenticated number.

  Note: You use authenticate one or more of a user’s numbers via the User dialog. See “The User \ Numbers tab” on page 11-26.

- **Allow administrator login**. Select this checkbox to allow a Wave administrator to call into this auto attendant and manage its greetings over the phone, including listening to the greetings, re-recording an existing greeting, recording a new greeting, making a different greeting active, and deleting a greeting.

  Note: You must add an “Auto attendant configuration” menu choice to the auto attendant to support administrator login. When the administrator selects that menu choice, he or she is prompted to enter the password you specify here, and then hears a menu of greeting management options. See “Defining menu choices” on page 13-6.

  Password/Confirmation. Enter and confirm the password required to log on.

7. Click **OK** or proceed to the next section.

Defining menu choices

An auto attendant can present a series of menu choices to callers. For example, callers might be prompted to press 1 to transfer to the Sales department, 2 to transfer to the Customer Service department, and so forth. When a caller reaches an auto attendant, the auto attendant's greeting plays, followed by its menu choice prompts in the order you specify.

Caution! *If your auto attendant supports extension dialing, try to avoid menu choices conflicting with extension numbers. For example, if you assign the 2 key to a menu choice, consider avoiding extensions beginning with 2. Otherwise callers trying to dial the extension might select the menu choice instead.*

Each menu choice can contain the following:

- **Prompt**. Recorded message that explains the option to the caller. For example, "For Sales, press 1."
- **Key**. Phone key callers must press to select the option.
- **Action**. Action the system takes when the key is pressed.
- **Language**. Language for subsequent system prompts. When callers enter the key associated with this menu choice, all subsequent prompts are in the specified language. You can choose from the languages that are currently installed on the Wave Server. (See "Setting up system-wide audio options" on page 4-18 for more about how to install additional languages.)
- **Custom data and skill requirements**. Extra information attached to the call. Whenever a caller selects the menu choice, you can attach custom data variables and/or Contact Center queue agent skill requirements with the values you define. These values can be seen by users or used to automate call handling.

  Note that you can also attach custom data variables and skill requirements at the auto attendant level, as opposed to the menu choice level described here. See "Setting up custom data and skill requirements for an auto attendant" on page 13-22.

Menu choice actions

The following table lists the actions that you can choose.

Action	Description
Transfer to user	Transfers the call to the user that you specify.
Send to voicemail	Transfers the call to the voice mailbox of the user that you specify.
Play message	Plays a message that you record using the audio controls.
User login	Offers the caller the Wave login prompt to the Voicemail/account menu, letting the caller check voicemail and change account settings.
Dial by name	Offers callers the dial-by-name directory.
Jump to auto attendant	Transfers the call to another auto attendant that you specify. (See “When a call may be disconnected automatically” on page 13-8 for a special case.)
Transfer to Queue	Transfers the call to the Contact Center queue that you specify.
Transfer to Hunt Group	Transfers the call to the hunt group you specify. See “Configuring hunt groups of extensions” on page 10-43.
Auto attendant configuration	Allows a Wave administrator to manage this auto attendant’s greetings over the phone, including listening to the greetings, re-recording an existing greeting, recording a new greeting, making a different greeting active, and deleting a greeting. When the administrator selects this menu choice and enters the required password, he or she hears a menu of greeting management options. To access this feature, you must enable administrator login and provide the required password on the General tab of the Auto Attendant dialog.

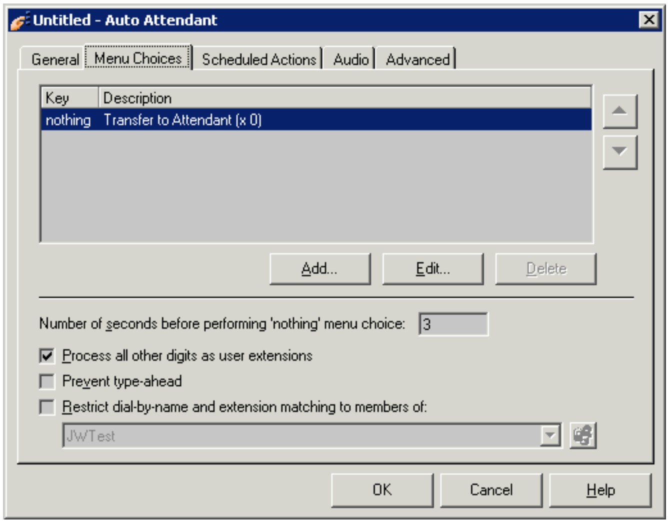
When a call may be disconnected automatically

The system automatically disconnects a call if the caller does not press a key during 3 consecutive jumps between auto attendants. This situation could occur if you if you configured an auto attendant's **Nothing** menu choice to perform the **Jump to auto attendant** action and then specified the same auto attendant. After 3 jumps without selecting a menu choice, the caller is presumed to have hung up.

Adding a menu choice

1 In the User/Group Management applet, in the Auto Attendants view create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.

2 Click the Menu Choices tab.



Untitled - Auto Attendant

Key	Description
nothing	Transfer to Attendant (x 0)

Number of seconds before performing 'nothing' menu choice: 3

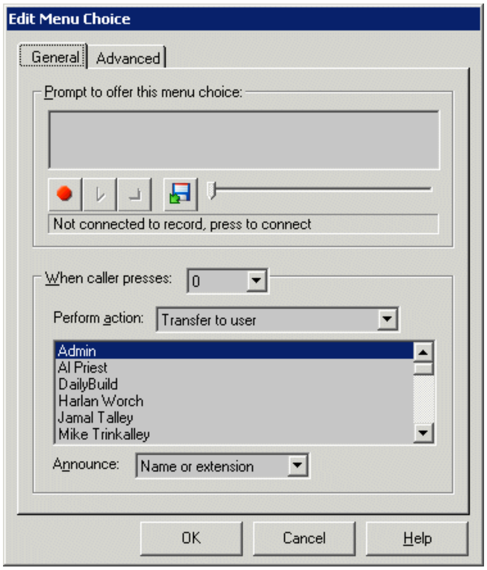
☑ Process all other digits as user extensions

☐ Prevent type-ahead

☐ Restrict dial-by-name and extension matching to members of:

JWTest

3 Click **Add** to create a new menu choice, or click **Edit** to modify the selected menu choice. The Edit Menu Choice dialog opens.



Prompt to offer this menu choice:

Not connected to record, press to connect

When caller presses: 0

Perform action: Transfer to user

Admin
Al Priest
DailyBuild
Harlan Worch
Jamal Talley
Mike Trinkalley

Announce: Name or extension

4 On the General tab, type the text of the Prompt to offer this menu choice, for example, “For Sales, press 1.” Use the audio controls to record a new prompt or import a WAV file containing the prompt. (See “Using the audio controls” on page 2-21.)

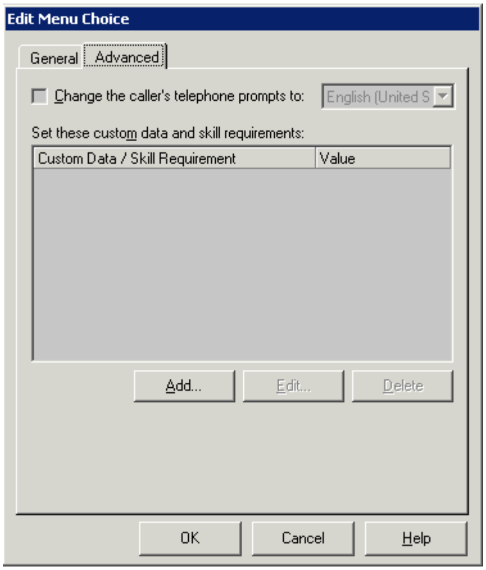
5 In **When caller presses**, select the key that callers must press to select the menu choice. Valid keys are 0-9, *, or #.

6 In the **Perform action** drop-down list, select the action to perform when callers press the key.

For transfers to a user, IVR Plug-in, or queue, select an optional Announce prompt, which determines what callers hear when they select this menu choice:

- **Nothing**. The call is transferred with no announcement.
- **Name or extension**. Announces the name of the user, IVR Plug-in, or queue, using the voice title if available. If no voice title is available, the auto attendant announces the extension to which the call is transferring.
- **One moment please**. Announces “One moment please” as the call is transferred.

7 Click the Advanced tab.



Edit Menu Choice

General | Advanced

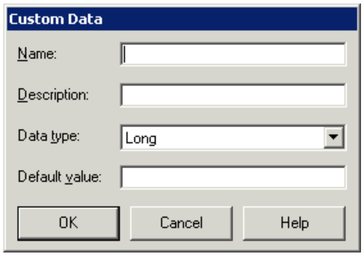
□ Change the caller's telephone prompts to: English (United S

Set these custom data and skill requirements:

Custom Data / Skill Requirement	Value

8 To change the language of subsequent prompts, check **Change the caller's telephone prompts to** checkbox. Then select another language from the drop-down list. When callers press the key for this menu choice, all subsequent prompts are in the language you specify here.

9 To set the value for one or more custom data variables or Contact Center queue skill requirements whenever this menu choice is selected, click **Add**. The Custom Data / Skill Requirement dialog opens.



Custom Data

Name:

Description:

Data type: Long

Default value:

- To attach a custom data variable to the call when this menu choice is selected, click **Custom data**, select the variable from the drop-down list, then enter the value to be assigned to the variable when the menu choice is selected. To create a new custom data variable, click ☆.
- To attach an agent skill requirement to the call when this menu choice is selected, click **Agent skill** and then select the skill from the drop-down list. To create a new skill, click ☆.

  For **Minimum value** and **Maximum value**, enter the range (from 0 to 100) that an agent's skill value must be within to qualify for taking the call.

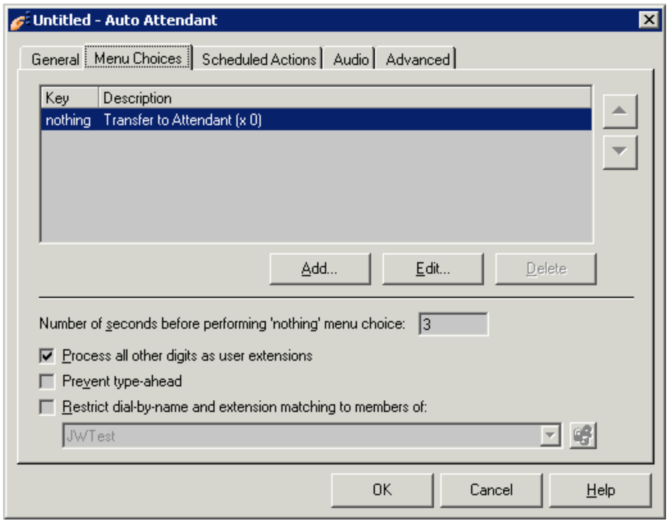
Custom data variables stay attached to the call as long as it remains within the original Wave where it was attached and are historically logged. For complete information on creating custom data variables and Contact Center skill requirements, see the *Wave Contact Center Administrator Guide*.

10. Click **OK** to return to the Edit Menu Choice dialog.
11. Click **OK** to save the menu choice and return to the Auto Attendant dialog.
12. On the Menu Choices tab, use the arrows to change the order in which menu choices are presented to callers.
13. Add more menu choices or click **OK** to save the auto attendant.

Setting general menu options

1 In the User/Group Management applet, in the Auto Attendants view create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.

2 Click the Menu Choices tab.



Key	Description
nothing	Transfer to Attendant (x 0)

Number of seconds before performing 'nothing' menu choice: 3

☑ Process all other digits as user extensions

□ Prevent type-ahead

□ Restrict dial-by-name and extension matching to members of:

JWTest

3 In **Number of seconds before performing 'nothing' menu choice**, enter the number of seconds that the auto attendant will wait without a menu choice being selected, before performing the action associated with the **Nothing** menu choice. The wait begins after the final menu choice prompt finishes playing. You can choose the action for the **Nothing** menu choice using the following steps.

4 To permit callers to dial other extensions while in this auto attendant, select the **Process all other digits as user extensions** checkbox (the default setting).

Note: Some extensions cannot be dialed from an auto attendant. If a caller enters the dial-by-name directory extension (the default is 411) or the extension of another auto attendant (for example, 560 for the default auto attendant), the caller hears "That extension does not exist" and the call is not transferred. (The same prompt is played if the caller enters an invalid extension.)

5 To disable type-ahead for this auto attendant, check **Prevent type-ahead**.

Type-ahead enables users to enter a sequence of commands together. For example, with a series of auto attendants set up as submenus, a caller could press 123 to choose menu choice 1, menu choice 2 from the submenu, and menu choice 3 from the final submenu. The problem with type-ahead is that if a caller enters a non-existent extension (for example, 123), the auto attendant processes the digits as type-ahead commands and sends the user to the appropriate menu or submenu. With type-ahead disabled, callers dialing non-existent extensions are never sent to menu choices. However, callers selecting menu choices must wait until they hear the prompts for each menu before entering commands for that menu.

6 To dedicate this auto attendant to a ViewPoint Group, so that only users in the Group can be dialed from it, check **Restrict dial-by-name and extension matching to members of**, and select the ViewPoint Group.

Customizing login behavior from auto attendants

By default, the **User login** menu choice prompts for extension and password, then sends users to Wave's voicemail/account menu (see Appendix A of the *Wave ViewPoint User Guide* for details). However, you can customize the user login destination, so that users who successfully log in are sent to a specific extension.

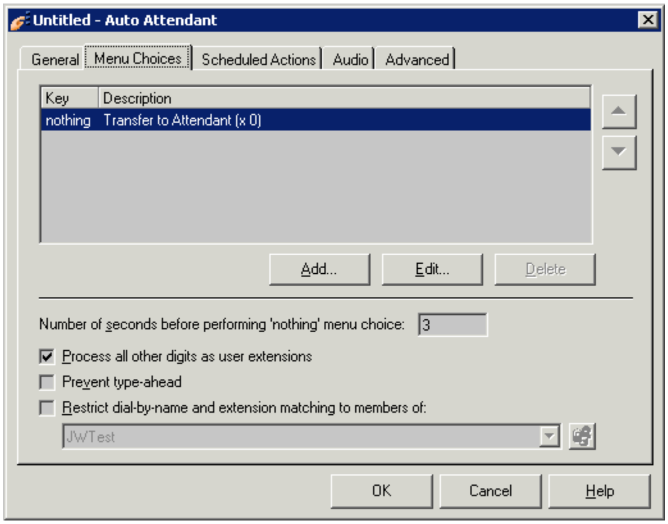
Note the following:

- When sending login calls to a custom destination, the standard Wave alert prompts do not play, for example the prompts alerting the user to DND status, active call forwarding, and nearly full voice mailbox. However, the user still is prompted to change his or her password if that is required.
- Customizing user login changes the login behavior through this auto attendant only. Users logging in from a station's dial tone always have the default behavior.

To customize user login

1 In the User/Group Management applet, in the Auto Attendants view create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.

2 Click the Menu Choices tab.



Key	Description
nothing	Transfer to Attendant (x 0)

Number of seconds before performing 'nothing' menu choice: 3

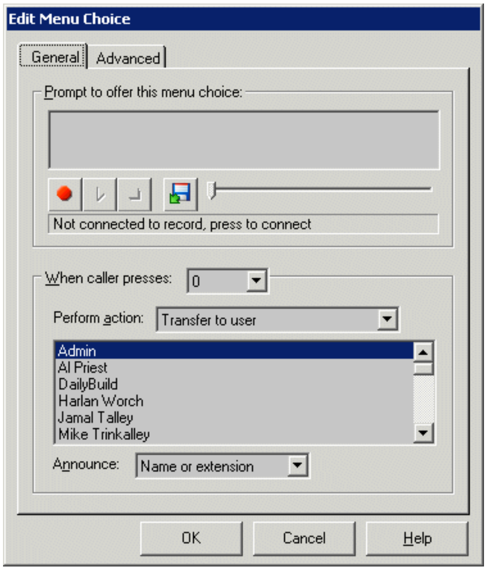
☑ Process all other digits as user extensions

☐ Prevent type-ahead

☐ Restrict dial-by-name and extension matching to members of:

JWTest

3 Click **Add**. The Edit Menu Choice dialog opens.



Edit Menu Choice

Prompt to offer this menu choice:

Not connected to record, press to connect

When caller presses: 0

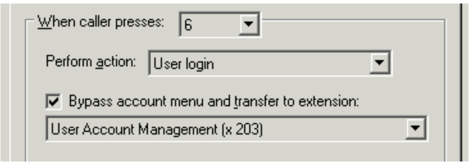
Perform action: Transfer to user

Admin
Al Priest
DailyBuild
Harlan Worch
Jamal Talley
Mike Trinkalley

Announce: Name or extension

4 In **When caller presses**, select the key that callers must press to select the menu choice to login from the auto attendant. Valid keys are 0-9, *, or #.

5 From the **Perform action** drop-down list, select **User login**.



When caller presses: 6

Perform action: User login

☑ Bypass account menu and transfer to extension:

User Account Management (x 203)

6 Select the **Bypass account menu and transfer to** and then select the destination extension from the drop-down list.

7 Click **OK**.

Avoiding the auto attendant ambiguous dialing delay

By default, when a caller dials an ambiguous number at an auto attendant, there is a 3-second delay while the system waits to see if the number is complete. For example, if the auto attendant has a menu choice accessed by pressing 2, and an extension 200, a caller pressing 2 will experience the delay while the auto attendant waits to see if more digits are coming.

You can bypass or change the delay in the following ways:

- The caller can press # after dialing the number. This signals that the number is complete, and the caller is connected without delay.
- You can modify your dialing plan to eliminate ambiguous numbers.
- You can turn off extension dialing, if the auto attendant is meant to be used only for menu choices. To do so, uncheck **Process all other digits as user extensions** on the Menu Choices tab. This bypasses any ambiguities between menu choices and extension numbers, enabling menu choices to be dialed without the delay.
- You can modify the length of the delay by changing the Wave Advanced Setting `AutoAttendantInterdigitTimeout`. Be careful when modifying this setting if ambiguous numbers exist, because callers may find themselves connected to the wrong number.

Scheduling transfers and greetings

You can customize an auto attendant to automatically change its behavior based on time of day or on special dates. You can schedule the following actions:

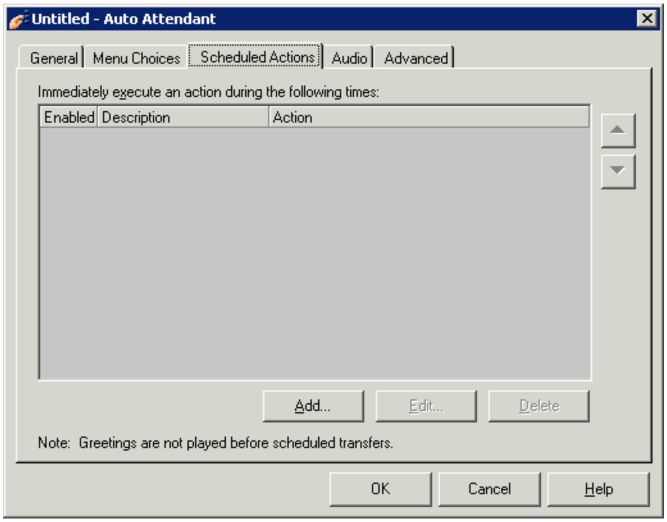
- Playing of a different main greeting, which replaces the auto attendant’s regular greeting. For example, you can schedule a “We’re closed” greeting to be played to all callers after business hours and on weekends.
- A transfer to any other extension, including another auto attendant, user, queue, hunt group, or ViewPoint Group. For example, to provide extended customer support coverage, support calls that arrive after your California office closes in the evening can transfer automatically to the main auto attendant at your facility in New Zealand.

Note: If you have scheduled a greeting and a transfer to occur at the same time, the transfer always takes precedence and the greeting does not play. Also, if you have two greetings or two transfers scheduled for overlapping times, the top-most scheduled item always takes precedence.

To schedule transfers or greetings

1 In the User/Group Management applet, in the Auto Attendants view create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.

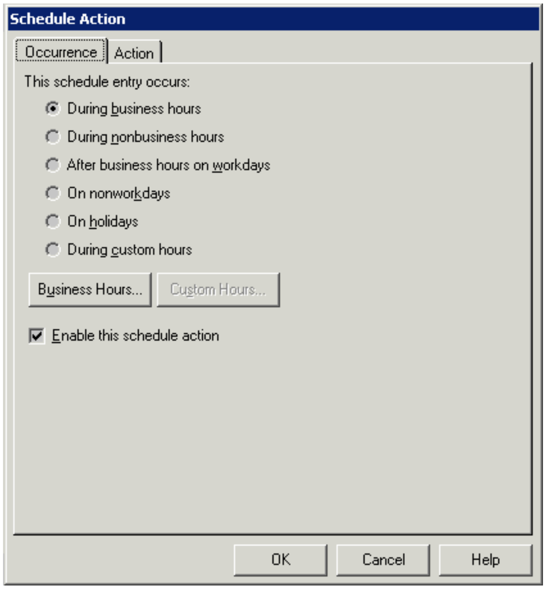
2 Click the Scheduled Actions tab.


Untitled - Auto Attendant
General
Menu Choices
Scheduled Actions
Audio
Advanced
Immediately execute an action during the following times:
Enabled
Description
Action
Add...
Edit...
Delete
Note: Greetings are not played before scheduled transfers.
OK
Cancel
Help

The following table shows the information that is displayed for each scheduled action already defined for this auto attendant.

Column	Description
Enabled	If checked, the action will be performed as scheduled. If unchecked, the action is temporarily disabled.
Description	Time period during which the action will be performed.
Action	Action that will be performed.

3 Click **Add** to schedule a new action, or click **Edit** to modify the selected action. The Schedule Action dialog opens.



Schedule Action

This schedule entry occurs:

● During business hours
○ During nonbusiness hours
○ After business hours on workdays
○ On nonworkdays
○ On holidays
○ During custom hours

☑ Enable this schedule action

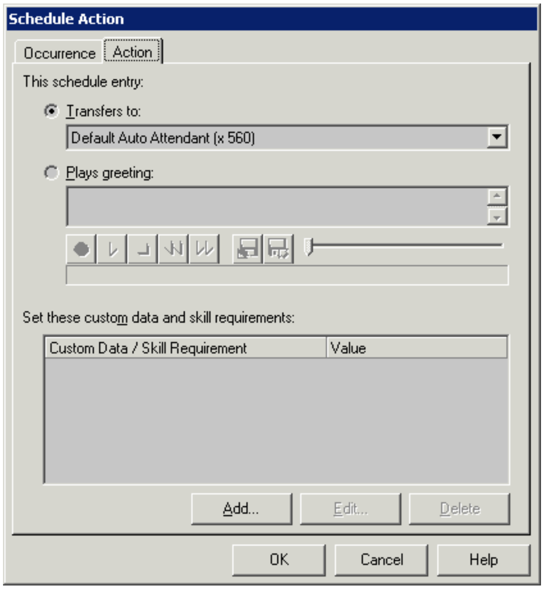
4 On the Occurrence tab, select one of the periods of time during which the action will occur.

Note: If your system uses several sets of business hours, click Business Hours before you click **OK** in the Schedule Action dialog and verify that the action will take place according to the set of business hours that you want to use.

If you choose During custom hours, click Custom Hours and set your hours in the dialog that opens.

5 Check **Enable this schedule action** to activate this action as soon as you save the auto attendant. If unchecked, the action is temporarily disabled.

6 Click the Action tab.



Schedule Action

This schedule entry:

● Transfers to: Default Auto Attendant (x 560)

○ Plays greeting:

Set these custom data and skill requirements:

Custom Data / Skill Requirement	Value

7 Under **This schedule entry**, select the action that the auto attendant will perform immediately when a call arrives during the period covered by the schedule entry:

- **Transfers to**. Immediately transfers callers to the extension that you select from the drop-down list during the scheduled time period.
- **Plays greeting**. Immediately plays the greeting that you record during the scheduled time period.

8 Using the **Set these custom data and skill requirements** section, you can have the auto attendant automatically attach custom data variables or apply skill requirements to all calls handled by the schedule rule.

9 Click **OK**. The Schedule Action dialog closes.

10 On the Scheduled Actions tab in the Auto Attendant dialog, use the arrows to move a scheduled transfer or greeting to a different position on the list. If you have two greetings or two transfers scheduled for overlapping times, the one that is at the top of the list will be used. If a greeting and a transfer are scheduled for the same time, the greeting is not played.

11 Click **OK** in the Auto Attendant dialog to save your changes.

Setting up an auto attendant's hold music and greetings

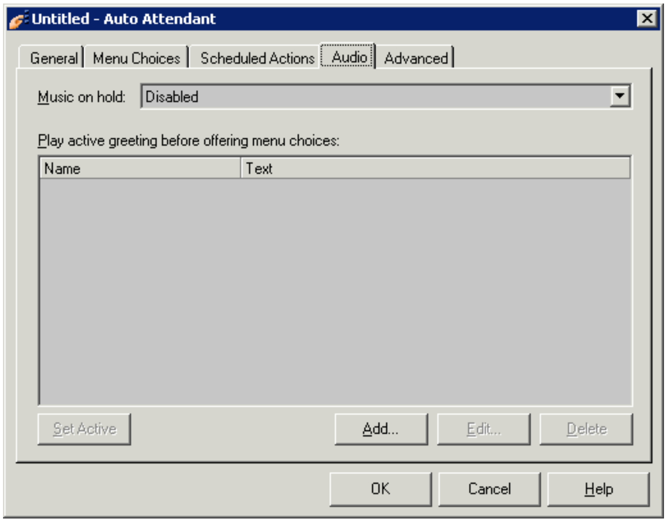
You use this tab to do the following:

- **Configure a music-on-hold source for the auto attendant.** Each auto attendant can have its own music-on-hold source as described below, or default to the system source (see "Configuring Music On Hold" on page 16-21.). A caller hears this music while the auto attendant is transferring him or her to an extension and continues to hear it while on hold until reaching a part of Wave that uses different hold music, such as a Contact Center queue or another auto attendant that has different hold music settings.
- **Record greetings for the auto attendant.** You can record multiple greetings for an auto attendant for use at different times of day, after hours, on holidays, and so forth, and make any one of them the active greeting.

To set up hold music and greetings for an auto attendant

1 In the User/Group Management applet, in the Auto Attendants view create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.

2 Click the Audio tab.



Untitled - Auto Attendant

Music on hold: Disabled

Play active greeting before offering menu choices:

Name	Text

3 Select the **Music on hold** source you want to use for this auto attendant from the drop-down list.

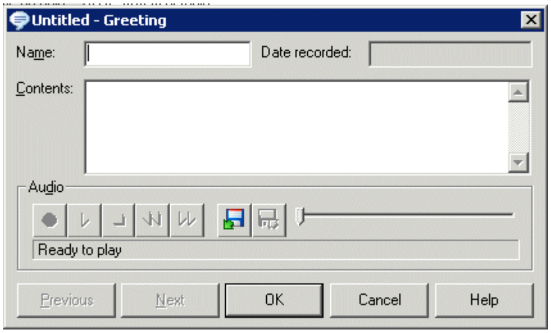
- **(Use system default)**. Use the system-wide hold music source as specified in the General Settings applet.
- **Disabled**. Do not play music to callers on hold.

  Hint: It is highly recommended that you specify a music-on-hold source or use the system default so that a caller does not hear extended ringing or silence, which may result in a hang-up.

- **External (Audio Input Jack)**. Play hold music from an external device, typically a CD player, radio, or specialized music-on-hold device.
- **Song n (<song title>)**. Play the selected WAV file to callers on hold.

Note: The system default music-on-hold source (if specified) as well as the other items listed in this drop-down list are set up via the General Settings applet. For more information, see "Configuring Music On Hold" on page 16-21.

4 To record a new greeting to be played to callers who reach the auto attendant, click **Add**. (To re-record an existing greeting, select it and click **Edit**.) The Greeting dialog opens.


Untitled - Greeting

Name:

Date recorded:

Contents:

Audio

Ready to play

5 Enter the following information about the greeting:

- **Name**. Greeting name, for example "After Hours - Holiday Season".
- **Contents**. Text of the greeting or a description of it, for example "Includes extended holiday shopping hours".

The date and time when the greeting was recorded or last edited is displayed in the **Date recorded** field.

6 Use the audio controls to record the greeting. (See “Using the audio controls” on page 2-21.)

7 Click **OK** to save the greeting. The new greeting is added to the list of all greetings that have been recorded so far.

8 Select a greeting and click **Set Active** to make it the active greeting to be played when a caller reaches this auto attendant, before any of the auto attendant’s menu choices are played to the caller.

9 Click **OK**.

Setting up custom data and skill requirements for an auto attendant

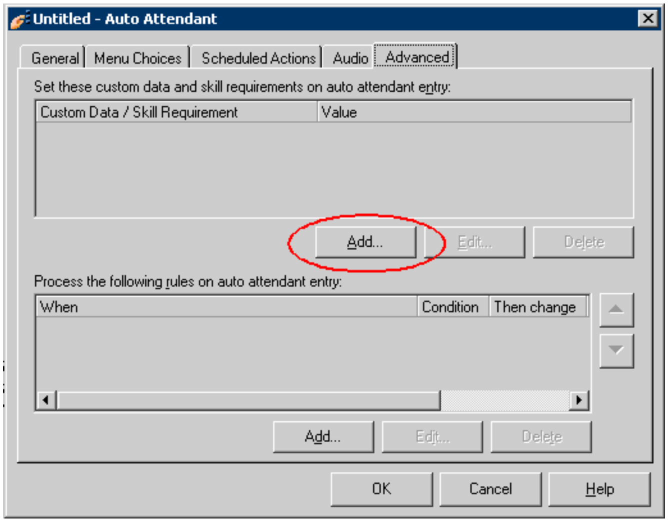
Custom data and skill requirements are extra information attached to a call. Whenever a call is handled by the auto attendant, you can attach custom data variables and/or Contact Center queue agent skill requirements to the call with the values you define. These values can then be seen by users or used to automate call handling.

Note: You can also attach custom data variables and skill requirements at the menu choice level, as opposed to the auto attendant level described here. See “Defining menu choices” on page 13-6.

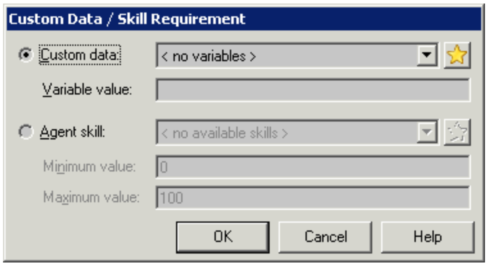
To set up custom data or skill requirements for an auto attendant

1 In the User/Group Management applet, in the Auto Attendants view create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.

2 Click the Advanced tab. To set the value for one or more custom data variables or Contact Center queue skill requirements whenever this auto attendant handles a call, click **Add**.


Untitled - Auto Attendant
General
Menu Choices
Scheduled Actions
Audio
Advanced
Set these custom data and skill requirements on auto attendant entry:
Custom Data / Skill Requirement
Value
Add...
Edit...
Delete
Process the following rules on auto attendant entry:
When
Condition
Then change
Add...
Edit...
Delete
OK
Cancel
Help

3 The Custom Data / Skill Requirement dialog opens.



- To attach a custom data variable to all calls handled by this auto attendant, click **Custom data**, select the variable from the drop-down list, then enter the value to be assigned to the variable when the menu choice is selected. To create a new custom data variable, click ☆.
- To attach a Contact Center queue skill requirement to all calls handled by this auto attendant, click **Agent skill** and then select the skill from the drop-down list. To create a new skill, click ☆.

  For **Minimum value** and **Maximum value**, enter the range (from 0 to 100) that an agent's skill value must be within to qualify for taking the call.

For complete information on creating custom data variables and Contact Center skill requirements, see the *Wave Contact Center Administrator Guide*.

Deleting an auto attendant

To delete an auto attendant, in the User/Group Management applet, right-click the auto attendant and then select **Delete**.

Important! A warning is displayed if you try to delete an auto attendant that is currently being used as a target location of any kind, for example "This auto attendant is currently being used as a routing list target: [Name] (extension). Edit or delete these locations before deleting this auto attendant."

The warning is displayed if you try to delete an auto attendant that is currently being used as any of the following:

- Forward-to extension: [Name] (extension)
- Intercept destination: [Name] (Trunk Group)
- Also ring extension: [Name] (Trunk Group)
- Call notification: [Name] (extension, Cascading Notification Rule: [Rule Name])
- Call notification: [Name] (extension)
- Routing List target: [Name] (extension)
- Menu choice for Auto Attendant: [AA Name] extension)
- ViewPoint group member: [Group Name]
- Operator: [Name] (extension)

Configuring the trunk group for the auto attendant extension

After creating auto attendants, or even if you are using only the default auto attendant, you should configure the Trunk Group to correctly route the auto attendant extension.

There are some advanced uses for auto-attendants that may not require that they be routed through a trunk group, for example internal auto-attendants, auto-attendants that route to other auto-attendants, auto-attendants that are scheduled in other auto-attendants, and so forth.)

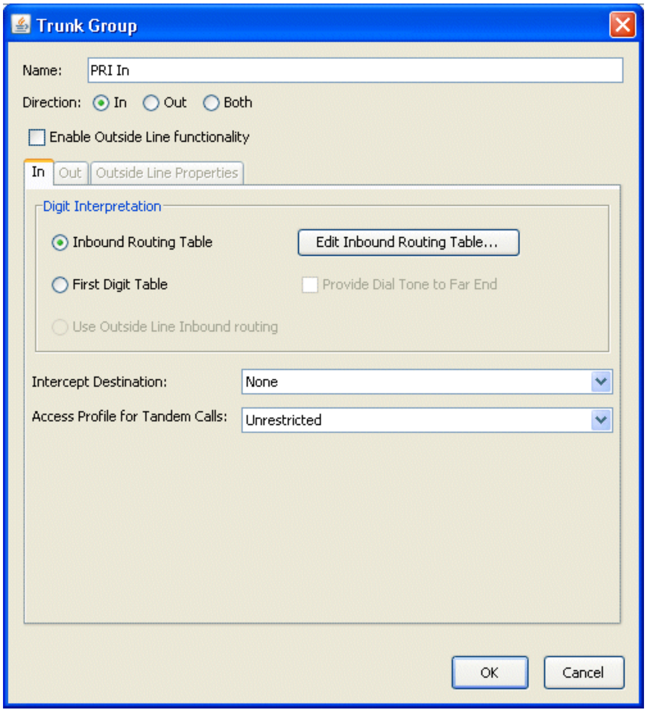
To configure the trunk group for an auto attendant

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Groups icon, located in the Trunk Administration section. The Trunk Groups dialog opens.

3 Select the trunk group you are using for phone lines, and then click **Edit**. The Trunk Group dialog opens at the In tab.


Trunk Group

Name: PRI In

Direction: ● In ○ Out ○ Both

□ Enable Outside Line functionality

In | Out | Outside Line Properties

Digit Interpretation

● Inbound Routing Table

○ First Digit Table

○ Use Outside Line Inbound routing

□ Provide Dial Tone to Far End

Intercept Destination: None

Access Profile for Tandem Calls: Unrestricted

4 Choose one of the following methods to route calls to the auto attendant:

- For simple routing, set **Intercept Destination** to the auto attendant.
- For scheduled routing, click **Edit Inbound Routing Table**, click **Add**, and in the **Destination** cell enter the auto attendant's extension. Then use the other fields to set route calls according to the schedule you want.

For more information about the Inbound Routing table, see "Configuring inbound routing tables" on page 8-4.

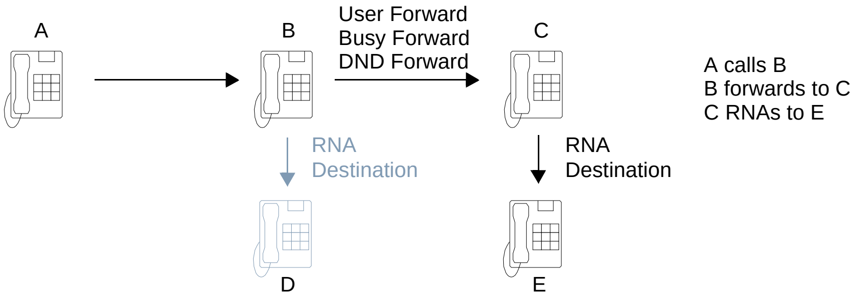
5 Click **OK** until you return to the Management Console.

Configuring calls to be forwarded to the RNA forwarding target

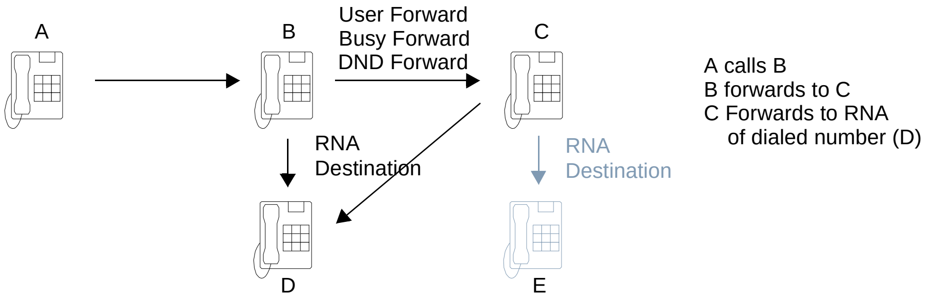
Click

Select the **Use Forwarding Target of Last Destination in Chain** check box in the General Settings applet, PBX (Advanced) tab to specify that calls are forwarded to the ring no answer (RNA) forwarding target of the last destination in a chain of calls.

The following illustration shows call flow if the **Use Forwarding Target of Last Destination in Chain** checkbox is selected:



The following illustration shows call flow if the **Use Forwarding Target of Last Destination in Chain** checkbox is not selected:



Note: Calls forwarded to Voice Mail are always forwarded to the Voice Mail of the dialed number.

To configure calls to be forwarded to the RNA destination of the last destination:

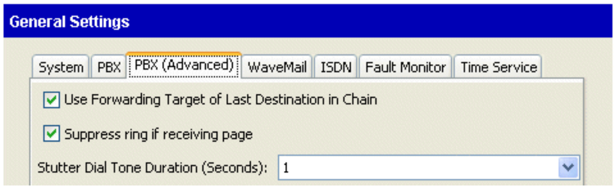
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the PBX (Advanced) tab.

4 Select the **Use Forwarding Target of Last Destination in Chain** check box.



General Settings

☑ Use Forwarding Target of Last Destination in Chain

☑ Suppress ring if receiving page

Stutter Dial Tone Duration (Seconds): 1

5 Click **Apply** to save your changes.

6 Click **Done** to return to the Management Console.

Chapter 14

Data Networking Configuration

Chapter Contents

Before you can configure your Wave Server to pass-through data channels from a T-1 line, you must have already configured your analog and digital trunks. (See Chapter 5, Configuring Analog and Digital Trunks..)

Ensuring that the T-1 serial interface is set correctly

When you connect an external router to your Wave Server's T-1 module with a serial interface, you must:

- Assign channels of the T-1 trunk to the serial interface (see "Assigning digital channels to a serial interface" on page 5-36 for details)
- Ensure the serial interface is set correctly

Typically, you will not need to change the interface settings unless you have a non-standard configuration.

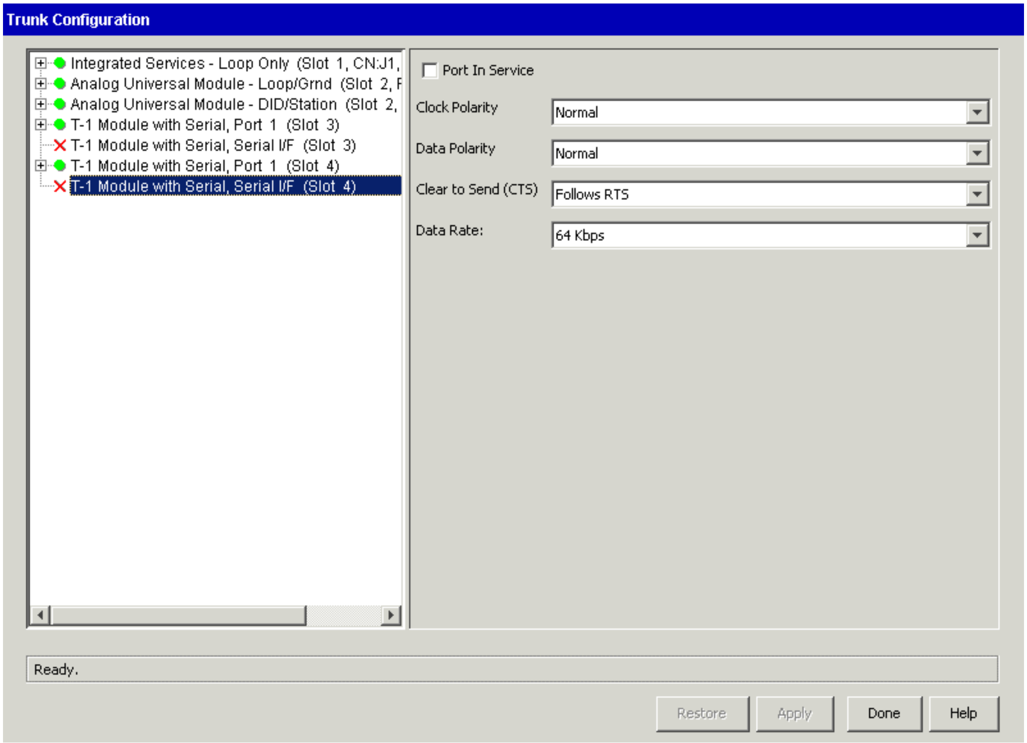
To ensure that the serial interface is set correctly

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Select the serial interface, labeled Serial I/F, and ensure that the settings are correct for your configuration.



Trunk Configuration

- Integrated Services - Loop Only (Slot 1, CN:J1,
- Analog Universal Module - Loop/Grnd (Slot 2, F
- Analog Universal Module - DID/Station (Slot 2,
- T-1 Module with Serial, Port 1 (Slot 3)
- T-1 Module with Serial, Serial I/F (Slot 3)
- T-1 Module with Serial, Port 1 (Slot 4)
- T-1 Module with Serial, Serial I/F (Slot 4)

□ Port In Service

Clock Polarity: Normal

Data Polarity: Normal

Clear to Send (CTS): Follows RTS

Data Rate: 64 Kbps

Ready.

- **Clock Polarity**. Normal is the default. You might change this setting if there is a lot of latency between the Wave Server and the external router, typically due to a long cable (more than 10 feet) between the two devices. The likelihood of this scenario is increased when more channels are used. If you see data errors, you might try inverting the clock.
- **Data Polarity**. Normal is the default. If you change this setting to Inverted, you must invert the data polarity on both ends of the connection.
- **Clear to Send**. Follow RTS (Request to Send) is the default. Set this to Always On, if the device at the other end of the connection is not driving RTS.
- **Data Rate**. 64 Kbps is the default. Do not change this setting to 56 Kbps unless you know your connection’s maximum data rate is 56 Kbps.

4 Click **Apply** to save your changes.

5 Click **Done** to return to the Management Console.

Chapter 15

Initial System Administration

Chapter Contents

This chapter guides you through the final tasks of initial system configuration.

- Backing up your Wave system configuration
- Mirroring your hard drive and RAID
- Restarting the Wave Server
- Running Microsoft Systems Management Server
- Imaging and restoring your system using Live Image

Backing up your Wave system configuration

You should back up your system:

- After you complete your initial configuration.
- Every time you make a configuration change.
- Whenever you perform a software upgrade or install third-party software.
- On a regular basis.

There are 2 ways to back up and restore your system:

- **Using Backup/Restore**. Backup/Restore backs up your Wave system configuration and other items, but does not back up your entire system.
- **Using the Wave Live Image Add-on**. Live Image creates a disk image backup of your entire Wave system. You use the Recovery Disk Creation utility to create a bootable USB device tat you can use to rebuild your Wave system from scratch or to return to a previous working version.

This section describes how to use Backup/Restore to backup your system configuration. See “Imaging and restoring your system using Live Image” on page 15-14 for information about using the Live Image Add-on.

Using Backup/Restore

Wave automatically runs Backup/Restore every night at 2:00 AM to back up the system configuration database file so that you can recover from situations where the database might be corrupted. Every time Wave restarts, the startup procedure checks the database for problems, and it is repaired or replaced with the backup copy if necessary.

The System Backup/Restore applet backs up the following items.

- **Wave configuration**, including database file and registry keys.
- **WaveNet databases**, if the Wave Server is a node in a WaveNet network. See “Special Backup/Restore considerations on a WaveNet node” on page 15-5 for more information.
- **RRAS configuration**.
- **Voicemail Greetings, Names, and Mailboxes directories**.

- **System prompts**. The default language set of system-wide prompts is automatically backed up. You specify the default language to use via the User/Group Management applet (**System Settings dialog > Audio tab > Default system prompts**.)

  Additional language versions of the system prompts will also be backed up automatically if you specify any of the following. (All of these language settings are specified via the User/Group Management applet.)

  - If you specify another language for a user or user template. See “Choosing a language for phone prompts” on page 11-89.
  - If you specify another language for an Auto Attendant’s menu choices. See “Adding a menu choice” on page 13-8.
  - If you specify another language for a Contact Center queue’s prompts. See “Choosing the language for a queue’s phone prompts” in Chapter 2 in the *Wave Contact Center Administrator Guide*.

  Note that if you have other languages installed but not specified in any of the ways listed above, additional versions of the system prompts in those languages are not backed up automatically.
- **Wave licensing information**.
- **Voicemail messages and Music On Hold WAV files** (optional).
- **Call Navigator prompts** (optional).

Caution! *The IP Address, Subnet Mask, and Gateway settings are also backed up, and will be applied if you restore to a different Wave Server. If you restore to a different Wave Server, you must set the appropriate IP Address, Subnet Mask, and Gateway on the new Server.*

The System Backup/Restore applet does not back up the following items:

- Network Adapters and Settings, including host name/machine name and TCP/IP domain.
- Password Administration settings (Wave account user names and passwords).
- Date and Time settings
- RAID settings (Windows Disk Management)
- Windows Workgroup or Network Domain settings

Note the following:

- Depending upon the number and size of your voicemail messages, the backup and restore procedure could each take up to 2 hours. For that reason, schedule backups during off-peak hours.
- Compression takes place only after a temporary full backup of the raw files has been created, so be sure that your Wave Server's hard drive has enough space (up to 2 GB) to accommodate the temporary backup files.
- You can only restore from a backup of a system of the same version number as your current system.
- Since the backup and restore procedure uses FTP, the client PC doing the backup must have an FTP program installed.

About very large backups

If your Wave database is very large, or you are recording calls but do not call recordings regularly, the backup file can grow beyond two GB. In this case, backups will take longer than 2 hours to complete and multiple 2 GB backup files will be generated as described below. To avoid this and keep your backup times reasonable, best practice is to archive off call recordings on a regular basis.

A system backup is written to a CAB file. When the backup CAB file size exceeds 2GB, a new CAB file is created. These sequential backup files will be named iobackup.cab, ioback2.cab, iobackup3.CAB and so on. The restore process will extract all the related CAB files in sequence.

Note: To restore your system from multiple CAB files, all the CAB files must be present in the same Windows folder.

Special Backup/Restore considerations on a WaveNet node

If you are backing up or restoring a system configuration on a Wave Server that is a node in a WaveNet network, note the important information in this section. (See Chapter Chapter 25 for complete information about using WaveNet.)

Warning! *Never restore a system configuration from one WaveNet node to another WaveNet node on the same network. Doing so will introduce inconsistencies in the network configuration, and the restored node will take the place of the backed-up node in the WaveNet network. Extensive manual re-configuration will be required to correct the network configuration.*

If a Wave Server was physically connected as a node in a WaveNet network when you backed up that Server's system configuration, make sure that the Server is still physically connected before you perform the restore so that the restored node is automatically re-synchronized with the other nodes in the network.

After the restore completes, the restored node sends a message to each other node and re-synchronizes based on the responses received. If the restored node is not connected to the network or cannot establish connectivity with one or more other nodes, those nodes will be removed from the WaveNet configuration on the restored node. If this occurs, the WaveNet configuration must be manually re-created.

Important! Be sure to verify connectivity before you perform the restore—there is a 10 minute window during which automatic re-synchronization is attempted. After 10 minutes, all of the other nodes are removed from the WaveNet configuration on the restored node. At that point, the WaveNet configuration must be manually re-created.

To verify that a Wave Server is physically connected to the WaveNet network

1. Make sure that the Wave Server to be restored is physically connected to the network via a network cable.
2. From the node to be restored, verify that you can successfully Ping at least one other node in the network.

Note the following:

- If a WaveNet node was not currently added to the WaveNet network at any time before or after performing a backup, restoring the system configuration on that node does not physically re-add the restored node to the WaveNet network.
- If a WaveNet node was not currently added to the WaveNet network when the backup was performed, but was added before the restore is performed, the restored node will not be re-added to the WaveNet network after the restore. To re-add the restored node to the network, from any node in the network perform the steps in “Adding a Wave Server to the WaveNet network” on page 25-14.

  In this case, publications from the other nodes to the restored node will be re-established, but publications from the restored node will have to be re-built manually, because they were not included in the backup.

Backing up your system configuration using Backup/Restore

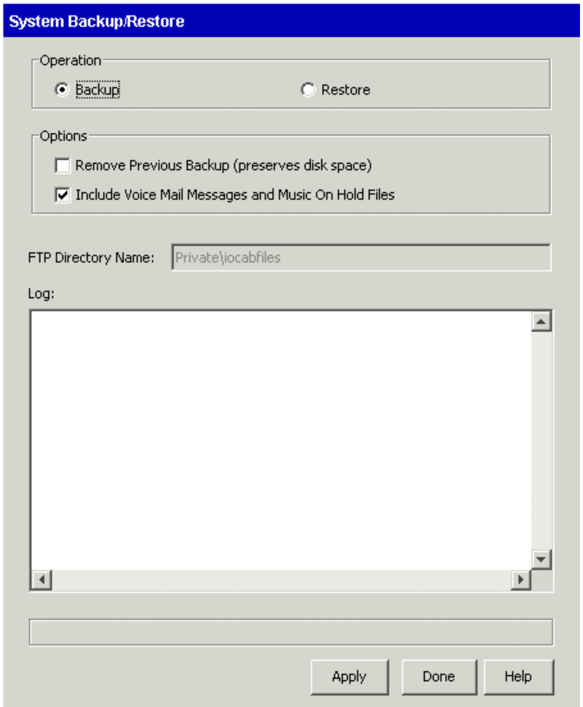
To back up your system configuration

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the System Backup/Restore icon, located in the General Administration section.

3 The System Backup/Restore dialog opens. If necessary, select **Backup**.



System Backup/Restore

Operation

● Backup ○ Restore

Options

□ Remove Previous Backup (preserves disk space)

☑ Include Voice Mail Messages and Music On Hold Files

FTP Directory Name: Private\iocabfiles

Log:

4 Click **Remove Previous Backup** to delete the previous backup file from Wave Server hard drive. (This option is disabled if no previous backup file is detected.)

5 Click **Include Voicemail Messages and Music On Hold Files** to back up voicemail messages and Music on Hold WAV files. Note that recorded names and greetings are included in the standard backup operation and are not affected by this option.

6 If you use the Call Navigator application and wish to back up its prompt files, select **Include Call Navigator Prompts**. (If Call Navigator is not installed on the Wave Server, this option does not appear.)

7 Click **Apply**.

Detailed results of the backup operation will appear in the Log field. The system configuration cabinet (CAB) file is stored in the following location:

```
C:\Inetpub\Ftproot\Private\Iocabfiles
```

Note: It is recommended that you transfer a copy of the CAB file to a different computer via FTP for safe storage.

8 Click **Apply** again.

9 Click **Done** to return to the Management Console.

Mirroring your hard drive and RAID

Important! The information in this section applies only to hard disk drives (HDDs)—NOT to solid state drives (SSDs). Since SSDs have no moving parts and are not susceptible to the types of problems that cause HDDs to fail, mirroring and RAID redundancy are unnecessary for SSDs.

As the last step of the initial configuration you should mirror your redundant hard drive using Windows Disk Management. This procedure creates a backup of your Wave configuration that you can fall back on in case of hard drive failure.

Redundant Array of Independent Disks, or RAID, brings another level of fault tolerance to the Wave Server. RAID is a set of disks (hard drives) that serve collectively as a single, logical storage device, providing data redundancy. The Disk Management application sets up disk mirroring, using one hard drive to mirror another with the same controller, so that an exact copy of the primary hard drive is stored on a secondary, mirrored hard drive.

Whenever you create a mirrored disk, you must use a hard drive of a size equal to or larger than the primary hard drive; the Disk Management application then creates a partition of the correct size automatically. It is best to use a new hard drive, preferably one that is identical to the primary hard drive. For consistency, obtain new hard drives from Vertical Communications.

Depending on the amount of data on the hard drive, it can take up to 30 minutes for Disk Management to mirror the Wave Server's `C:` drive.

Three scenarios are possible with Wave hard drives:

- A Wave Server purchased with two hard drives is preconfigured for RAID-1. The second hard drive is mirrored for you.
- If you add a second hard drive after you purchase a Wave Server, you need to configure RAID-1 on the second hard drive and mirror it. See the instructions below.
- If you need to recover a Wave system using a mirrored hard drive, you must break the mirror, power off the Wave Server, install the mirrored drive in slot A and insert a new drive in slot B, restart, and then mirror the new hard drive. See “Recovering with RAID-1 Configuration” on page 23-41.

Note the following:

- The hard drive labelled Disk 1 should be blank, unformatted, and partitionless. If the hard drive has partitions, delete the partitions before mirroring it. See “Clearing an old hard drive” on page 23-38.
- To view SNMP alarms while you are mirroring the hard drive, open another browser window on your workstation, log onto the Management Console, click the Administration tab if necessary, and click the SNMP Alarms icon. The SNMP Alarms applet reports the SNMP traps as they occur.

To mirror a new hard drive

1 Shut down the Wave Server.

2 Insert the new hard drive in slot B.

3 Restart the Wave Server.

4 Log on to the Management Console.

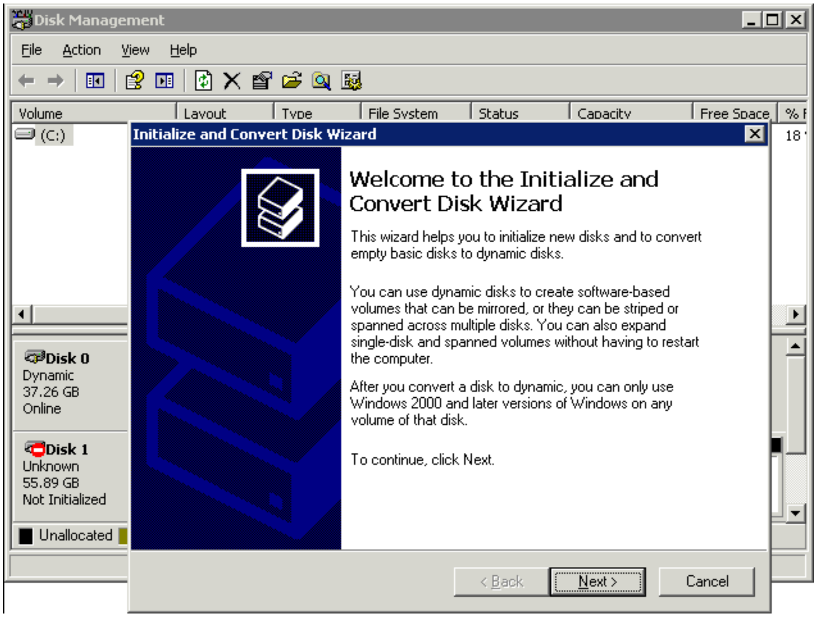
5 If necessary, click the Administration tab of the Management Console.

Click

6 Click the RAID-1 Configuration icon, located in the General Administration section.

7 If the new disk is not completely blank, the Disk Management applet opens. Go to step 10.

8 If the new disk is completely blank, the Initialize and Convert Disk Wizard starts automatically.



Welcome to the Initialize and Convert Disk Wizard

This wizard helps you to initialize new disks and to convert empty basic disks to dynamic disks.

You can use dynamic disks to create software-based volumes that can be mirrored, or they can be striped or spanned across multiple disks. You can also expand single-disk and spanned volumes without having to restart the computer.

After you convert a disk to dynamic, you can only use Windows 2000 and later versions of Windows on any volume of that disk.

To continue, click Next.

Disk 0
Dynamic
37.26 GB
Online

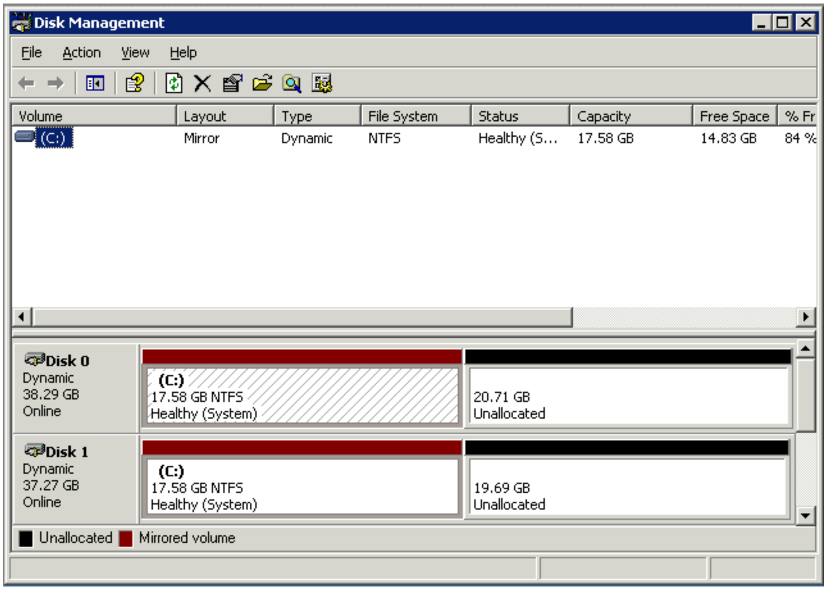
Disk 1
Unknown
55.89 GB
Not Initialized

Follow the on-screen instructions. Note the following:

- On the Select Disks to Initialize screen, verify that the new disk (“Disk 1”) is selected.
- On the Select Disks to Convert screen, select the checkbox to mark the new disk (“Disk 1”) for conversion to a dynamic disk.

9 Click **Finish**. Go to step 13.

10 In order to create a mirror of your hard drive, both disks must be dynamic disks. By default all drives are basic. To determine which format your disks are, look for either “Basic” or Dynamic” below the disk number.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Fr
(C:)	Mirror	Dynamic	NTFS	Healthy (S...	17.58 GB	14.83 GB	84 %

Disk 0
Dynamic
38.29 GB
Online

(C:)
17.58 GB NTFS
Healthy (System)

20.71 GB
Unallocated

Disk 1
Dynamic
37.27 GB
Online

(C:)
17.58 GB NTFS
Healthy (System)

19.69 GB
Unallocated

■ Unallocated ■ Mirrored volume

Important! If the secondary hard drive shows that it is "foreign", right-click in the space that says **Disk 1** and choose **Import foreign disk**. Disk 1 should now show "Online". Since Disk 1 must be empty before mirroring takes place, right click in the C: area for Disk 1 and choose **Remove volume**.

11 To convert your disks to dynamic disks, select the disk or disks at the bottom of the screen and select **Action > All Tasks > Convert to Dynamic Disk**.

12 Select the disks you want to convert, then click **OK**.

If you are converting Disk 0, follow the prompts to reboot your system. Once the system has been rebooted, log into the Management Console and re-enter the RAID-1 applet. You should now see that the disks are dynamic disks.

13 Click the `C:` partition on Disk 0.

14 Select **Action > All Tasks > Add Mirror**.

If the command is dimmed, your new hard drive is not blank. Follow the instructions in “Clearing an old hard drive” on page 23-38, then return to step 10.

15 Select Disk 1, then click **Add Mirror**.

A new color indicates mirroring (the default color is red).

Note: If the resulting mirrored partitions are of different sizes, then the primary and mirrored hard drives are physically incompatible. This should not happen if you received your hard drive from Vertical Communications. Contact technical support for assistance. While the mirroring will work, the mirrored hard drive will not boot if the primary hard drive fails; however, it will be recoverable from a separate machine.

The disks will now synchronize. Disk Management indicates initializing mirroring status with the following message:

RESYNCHING (percentage complete)

16 When mirroring is complete, Disk Management indicates healthy status with the following message:

HEALTHY

17 Exit Disk Management to return to the Management Console.

Note: If you remove the mirrored hard drive from the Wave Server and are running Wave with just the primary hard drive installed, be sure to return to the RAID-1 Configuration applet and break the mirror so that the system does not expect to see two hard drives.

RAID cautions

The following cautions apply to all situations using RAID:

- Do not change the Wave partition size. This will break the mirror and will cause both recovery and mirroring problems in the future.

  If the partition sizes are different after mirroring, the mirrored drive will not boot.

  It is not necessary to use Microsoft Windows formatting and partitioning features before you use the Disk Management application; the application performs all necessary steps for you.

- Do not attempt to mirror a Wave primary hard drive in Slot A onto a Wave primary hard drive in slot B. Due to the cloning technique used in manufacturing Wave primary drives, the Disk Management application cannot distinguish between primary drives.

  An alternative is to use Disk Management to remove all partitions on the second Wave primary disk so the disk will be treated as a new drive.
- Once you mirror a hard drive, either leave the mirrored hard drive in the slot or take it out and put it somewhere safe until you need it. If you take out the mirrored drive and are running with just one hard drive, break the mirror so that the system does not expect to see two hard drives.
- Do not use the mirrored hard drive as a primary hard drive and then load both hard drives back into the Wave Server. The system cannot distinguish between the two primary hard drives and will not be able to restart.
- You cannot see any SNMP alarms during RAID-1 configuration unless trap destinations are configured in the SNMP Configuration applet; for instructions, see “Configuring SNMP agents” on page 23-27.

Restarting the Wave Server

You will typically access the Restart Vertical Wave applet to restart remotely any time you change IP addresses, install new network services, change subnets, upgrade software, or install additional hardware.

A fully loaded Wave system can take up to 10 minutes to restart and come to a state where you can administer it remotely again. The duration of a restart is somewhat dependent on the routing functions you have enabled.

To restart a Wave Server remotely

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Restart System icon, located in the General Administration section.

3 In the **Seconds before restart** field, specify how many seconds should elapse before the system restarts.

4 Click **Restart** to restart the Wave Server.

5 Click **Yes** to confirm that you want to restart.

6 Click **OK**.

7 Close the browser window.

You cannot access the Wave Server until it is fully operational. If you are logging on remotely, you must wait a full 10 minutes before attempting to log on again. After a restart, use the Chassis View applet to verify that installed components are all working correctly.

Running Microsoft Systems Management Server

If you run Microsoft Systems Management Server (SMS) on your company network, configure the SMS software to exclude all Wave Servers from its control list.

Imaging and restoring your system using Live Image

Using the Wave Live Image Add-on, you can back up an image of the entire Wave Server, create a bootable USB drive, and then re-image the system in minutes instead of hours.

The Live Image Add-on is a separately-licensed application that allows you to schedule and perform disk image backups on a periodic (daily, weekly, and so forth) or one-time basis (for example, after initial system installation or after performing a major upgrade). An image backup task can perform a full backup every time it runs, or a full backup followed by a series of incremental backups that only contain changes since the last full backup.

The re-imaging process uses a bootable USB device that you create via the Recovery Disk Creation utility (a Windows stand-alone program included with Live Image). This recovery disk can then be used to boot a Wave Server in recovery mode to restore a previously-created backup image.

Live Image can dramatically reduce the time it takes to return to a fully-operational state after certain events, for example:

- After a catastrophic failure, you need to rebuild your system from scratch.
- After applying upgrades to a working system, you want to back out the changes to return to a working version.

Previously, you may have had to spend hours to recover the system, re-apply Service Packs and HotFixes as needed to bring your system up to the level it was at before the failure, and then restore the latest backup configuration in order to get up and running again. The time spent on this process could cause painful system downtime for end-user sites and lost revenue for dealers.

How Live Image works

When you perform an image backup, you store the backup image (TIB file) on a local hard drive on the Wave Server, on a hard drive in a USB enclosure, or on a network drive.

You then create a bootable USB device (either a USB flash drive or hard drive in a USB enclosure) using the Recovery Disk Creation utility. The Recovery Disk Creation utility does not automatically put the backup image file itself on the USB device. If the USB device is large enough, you can manually create the `Vertical\BackupImage` folder on the USB device and then copy the TIB file from the location where it was stored to that folder.)

To re-image your system, you insert the bootable USB device into the Wave Server. When you restart the Server, the system automatically searches for a backup image TIB file to use for re-imaging using the following search order.

- On the USB device itself in a folder called `Vertical\BackupImage`.
- On a hard drive connected to the Wave Server in a folder called `Vertical\BackupImage`. The hard drives are searched in reverse order, for example first the E drive, then D, C, and so forth.

The TIB file MUST be located in a folder called called `Vertical\BackupImage` in order to be found by the re-imaging process.

Important! Network drives are not included in the search, so if you store backup images on a network drive, be sure to copy the backup image file to use to a drive connected to the Wave Server (or to the USB device if it is large enough) before initiating the restart.

Note: If more than one backup image TIB file is found in the `Vertical\BackupImage` folder, if they are part of an incremental backup set, the latest one will be used. If they are separate image backups, whichever file is found first will be used. In order to prevent the wrong TIB file from being used, it is highly recommended that the `Vertical\BackupImage` folder ONLY contains the specific TIB file or files that are to be used to re-image your system if necessary, rather than using it as an interim storage location for various backups.

See the following:

- Installing Live Image. See page 15-17.
- Running Live Image. See page 15-17.
- Scheduling and performing a Live Image backup. See page 15-21.
- Preparing a bootable USB device using the Create Live Image Media utility. See page 15-25.
- Re-imaging your system using a Live Image backup file. See page 15-30.

Live Image requirements

- **Wave Live Image license**. If a valid Wave Live Image license is not installed on the Wave Server, you will not be able to run the Live Image Add-on or the Recovery Disk Creation utility.
- **Live Image HotFix**, if you are upgrading from Wave ISM 1.5 or 2.0. See “Installing Live Image” on page 15-17.
- **Additional Recovery Disk Creation utility requirements**:
  - Windows 7 or Windows Vista, base release or higher (32-bit and 64-bit versions)
  - .NET 4.0 or higher
  - USB device of 1 GB or larger. Note that 1 GB is required for the files and software to support the re-imaging. If you plan to copy the backup image file to the USB device as well, you will need a larger-capacity USB device.

    The following devices are supported when you create a bootable USB device:

    - USB flash drive
    - Hard drive in a USB enclosure

    Note: A list of supported USB devices is available on V-Connect. Choose **Products > Wave IP > Technical documents > Compatible USB Storage Devices for Live Image**.

Installing Live Image

Installing the Wave Live Image Add-on

- On a new system running Wave ISM 2.5 or higher, the Wave Live Image Add-on is installed automatically.
- If you are upgrading to Wave ISM 2.5 from Wave ISM 1.5 or 2.0, you install Wave Live Image via the LiveImage HotFix.

Live Image will be disabled until a valid Wave Live Image license is installed.

Installing the Recovery Disk Creation utility

Important! You install the Recovery Disk Creation utility on a separate PC that meets the requirements listed on page 15-16. You cannot install the Recovery Disk Creation utility on the Wave Server.

To install the utility, run the installer program located by default in the following location on the Wave Server:

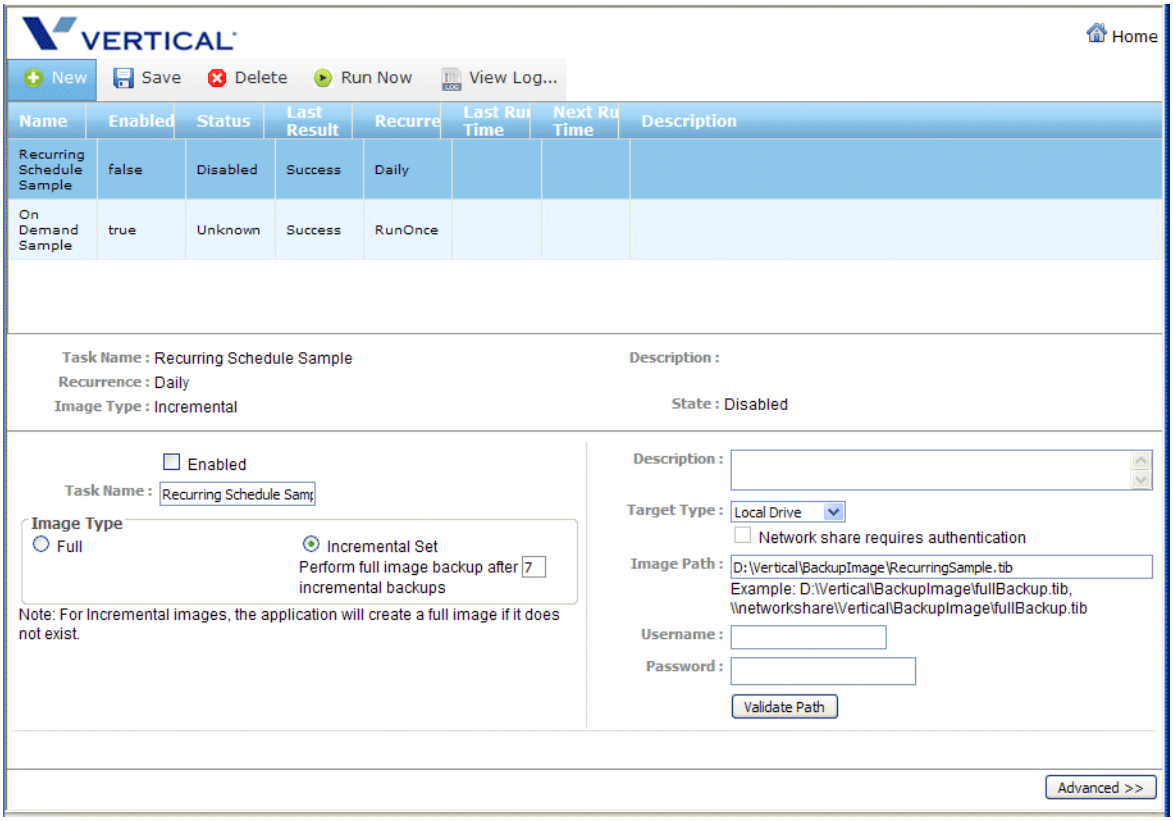
```
\Netsetup\CreateImageMediaSetUp.exe
```

Running Live Image

1. If you have not already done so, add and activate a Wave Live Image license. You cannot run Live Image without a valid license.
2. If necessary, click the Administration tab of the Management Console.
3. On the Administration tab of the Management Console, click the Live Image icon, located in the General Administration section.

Click

4 The Live Image web interface opens, displaying all image tasks that are currently in the schedule. The following example shows what you will see the first time you run Live Image—only the two sample image tasks included with Live Image are shown.



Name	Enabled	Status	Last Result	Recurre	Last Ru Time	Next Ru Time	Description
Recurring Schedule Sample	false	Disabled	Success	Daily			
On Demand Sample	true	Unknown	Success	RunOnce			

Task Name : Recurring Schedule Sample
Recurrence : Daily
Image Type : Incremental

Description :

State : Disabled

□ Enabled
Task Name : Recurring Schedule Samp

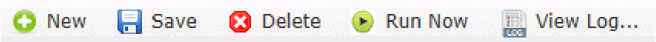
Image Type
○ Full
● Incremental Set
Perform full image backup after 7 incremental backups

Note: For Incremental images, the application will create a full image if it does not exist.

Description :
Target Type : Local Drive
□ Network share requires authentication
Image Path : D:\Vertical\BackupImage\RecurringSample.tib
Example: D:\Vertical\BackupImage\fullBackup.tib, \\networkshare\Vertical\BackupImage\fullBackup.tib
Username :
Password :

The screen is divided into the following sections:

- **Toolbar**. You use the Live Image toolbar at the top of the screen to perform the following tasks:

  - **New**. Creates a new image task.
  - **Save**. Saves any changes that you have made in the Task Details section.
  - **Delete**. Deletes the selected image task.
  - **Run Now**. Runs the selected image task immediately. Note that when you click **Run Now**, the status of the image task will not change until you click your browser’s Refresh button.
  - **View Log**. Displays the latest backup log for the selected image task.
- **Task Grid**. The Task Grid below the toolbar displays the following information for each image task:
  - **Name**. Descriptive name for the image task.
  - **Enabled**.
    - If **true**, the task is enabled and will run automatically at the scheduled times, if any have been specified. If the **Recurrence** for this task is set to **None**, the task will not run until it is manually executed by clicking **Run Now** on the Toolbar.
    - If **false**, the task is disabled and will not run. You can run the task at any time by clicking **Run Now** on the Toolbar.
  - **Status**. Current status of the image task:
    - **Running**. The task is currently executing.
    - **Ready**. The task is ready to be executed, but no instances are queued or running.
  - **Last Result**. The result of the image task the last time it ran—**Success** or **Failure**. Possible reasons for failure include:
    - **Failure**. Click **View Log** on the Toolbar for more information.
    - **Failure (No License)**. At the time the task last ran, the Live Image license was either not present, or it had expired.
    - **Failure (No Database Entry)**. The database information that corresponds to the Windows Scheduled Task does not exist. This message indicates an internal error or database problems.

        - **Failure (Invalid Disk Type)**. You specified a USB flash drive as the **Target type** the last time the task ran. Currently, only local hard drives, network drives, or hard drives enclosed in a USB enclosure are supported as targets for Live Image backups.
        - **Failure (Insufficient Disk Space or Access Denied)**. This error can occur when a target drive does not have sufficient free space to contain the image backup, or when, in the process of checking for available space on a network drive, it isn't possible to access the drive due to an invalid user id or password, insufficient permissions, network error, too many drives mapped, and so forth.

          Sufficient free space means that the target drive has at least the amount of free space available as is in use on the source drive. The same calculation is done for a full or an incremental backup.
        - **Failure (Invalid Command Parameters)**. This message indicates an internal error. Delete the task and recreate it; if the problem still occurs, contact Technical Support.
    - **Recurrence**. The frequency with which the image task will run, for example “Weekly”.
    - **Last Run Time**. The date and time the image task last ran. This column is blank:
        - If the task has never run.
        - If the task’s **Recurrence** is set to **Run Once** or **None**.
    - **Next Run Time**. The date and time when the image task is next scheduled to run. This column is blank:
        - If the task has never run.
        - If the **Enabled** checkbox is not selected.
        - If the task’s **Recurrence** is set to **Run Once** or **None**.
    - **Description**. Text description of the image task.
- **Summary section**. When you select an image task in the Task Grid, the details for that task are summarized in the Summary section below the grid. If you are creating a new image task, default values are displayed. In addition to some of the same fields described above for the Task Grid, the summary section also displays:
    - **Image Type**. If **Full**, the image task is a full backup of the Wave system. If **Incremental Set**, the image task is defined as a full backup followed by a number of incremental backups that you specify.

- **Task Details section**. When you select an image task in the Task Grid, that task’s details are displayed in the Task Details section at the bottom of the screen. If you are creating a new image task, default values are displayed. Task details are described in “Scheduling and performing a Live Image backup” on page 15-21.

Scheduling and performing a Live Image backup

Two sample image tasks are included with Live Image that you can modify or use as starting points for your own custom image tasks:

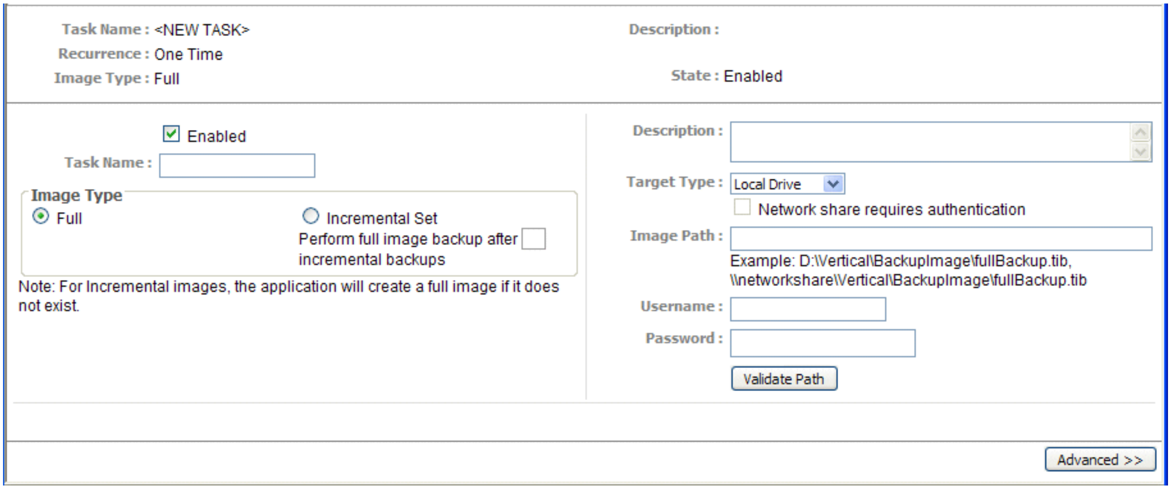
- **Recurring Schedule Sample**. This image task runs daily and performs an incremental backup. It is disabled by default.
- **On Demand Sample**. This image task runs on demand and performs a full backup. It is enabled by default.

Note: The sample tasks are for illustrative purposes only, and should not be expected to run successfully without modification. For example, the **Image path** in each sample task assumes a specific folder structure on a “D:\” drive on the Wave Server, which is unlikely to be present, even if you have a 2nd drive installed.

To create, schedule, and run a new image task

1 Click **New** on the toolbar.

2 In the Task Details section, enter the following information.



Task Name : <NEW TASK>
Recurrence : One Time
Image Type : Full
Description :
State : Enabled

☑ Enabled
Task Name :
Image Type
● Full
○ Incremental Set
Perform full image backup after □ incremental backups
Note: For Incremental images, the application will create a full image if it does not exist.

Description :
Target Type : Local Drive
□ Network share requires authentication
Image Path :
Example: D:\Vertical\BackupImage\fullBackup.tib, \\networkshare\Vertical\BackupImage\fullBackup.tib
Username :
Password :

- **Enabled**. If selected, this image task will run at the next scheduled time. If deselected, it will not run as scheduled.
- **Task Name**. Enter a unique descriptive name for the image task.
  - **Image Type**. Select one of the following:
    - **Full**. Performs a full backup of the entire Wave system.
    - **Incremental Set**. An incremental set consists of a full backup plus the number of incremental backups that you specify. Select this option to perform a full backup the first time the image task is run, followed by the number of incremental backups you specify below. When that incremental set is complete, the next set will start with a full backup again.
      - **Perform full backup after ___ incremental backups**. Number of incremental backups to perform before the next full backup. You can specify 1-99 incremental backups.

  Note: For incremental backups, Live Image will always create a full image if one does not exist.
- **Description**. Enter descriptive text about the image task.
- **Target Type**. Select one of the following destinations where the backup image will be saved:
  - **Local Drive**. Select the drive number of a local drive (or a hard drive in a USB enclosure). Do not specify a USB flash drive.
  - **Network Path**.
    - **Network share requires authentication**. This option is enabled only if you select a **Target Type** of **Network Path**. Select this checkbox if a valid username and password are required to save a backup image to the target location.
- **Image Path**. Enter the path and filename for the saved backup image.

  Important! You cannot specify a root-level image path. If you do, you will receive the error “Root directory cannot be used as a backup location”.
    - **On a local drive**. You cannot specify the image path `D:\backup.tib`. Use a secondary-level path instead, for example `D:\weeklybackup\backup.tib`.

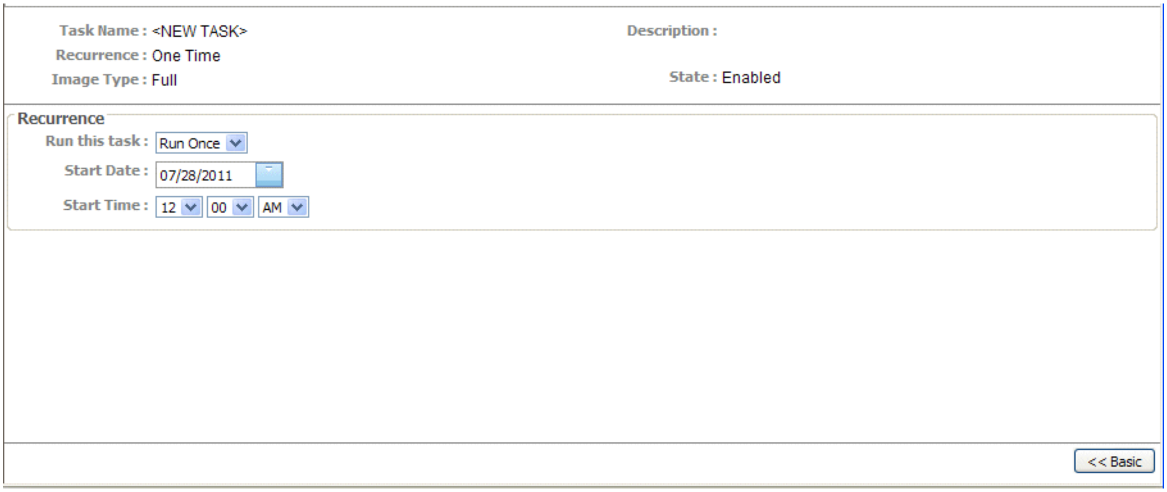
- **On a network drive**. You cannot specify a single-level folder for the image path. For example, you create a network share on computer “sstmaurice-ws” called “LiveImageWeeklyBackup” at `C:\LiveImageWeeklyBackup`. If you specify the image path “\\sstmaurice-ws\LiveImageWeeklyBackup \backup.tib”, you will receive the “Root directory cannot be used as a backup location” error.

  Instead, add a secondary folder level so that the image path is “\\sstmaurice-ws\LiveImageWeeklyBackup\weeklybackup\backup.tib.”

- **Username**. Enter the username required for network share access.
- **Password**. Enter the password required for network share access.
  - **Validate Path**. Click to test that the location you specified to save the backup image is accessible.

3 Click **Advanced** to add scheduling options to the image task. (Click **Basic** to return to the Task Details section.)

4 In the Recurrence section, enter the following information:

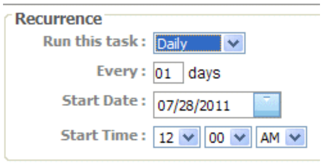


Task Name : <NEW TASK>
Recurrence : One Time
Image Type : Full
Description :
State : Enabled

Recurrence
Run this task : Run Once
Start Date : 07/28/2011
Start Time : 12 00 AM

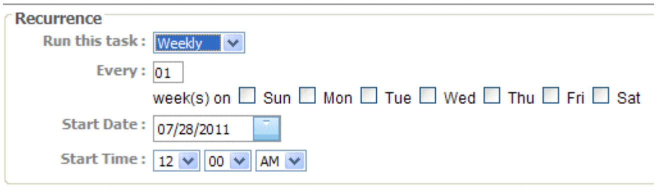
- **Run this Task**. Select one of the following from the drop-down list:
  - **None**. This image task is not scheduled and will not run until you click **Run Now** on the toolbar.
  - **Run Once**. This is an non-recurring scheduled image task that will run ONCE at the scheduled date and time. You can run it at any time by selecting it in the Task Grid and clicking **Run Now** on the Toolbar.

  - **Daily**. This image task runs automatically at the specified time and day-interval, for example at 10 PM every day, at 12:01 AM every third day, and so forth.
  - **Weekly**. This image task runs automatically at the specified time on the specified day of the week, for example at 5PM on Saturday.
  - **Monthly**. This image task runs automatically at the specified time on the specified day of the month, for example at 12:01 AM on the 15th day of every month.
- **Every** ___ . Determines how often the scheduled image task runs. (This field is hidden if you chose **None** or **Run Once** above.)
  - **Daily**. To run the image task every day, enter 1. To run the image task every other day, enter 2, and so forth.



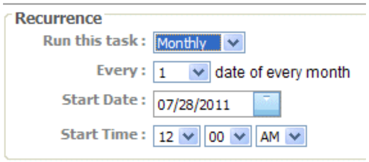
Recurrence
Run this task : Daily
Every : 01 days
Start Date : 07/28/2011
Start Time : 12 00 AM

  - **Weekly**. To run the image task every week, enter 1. To run the image task every other week, enter 2, and so forth. Then, select the day or days of the week on which the image task will run.



Recurrence
Run this task : Weekly
Every : 01
week(s) on □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Start Date : 07/28/2011
Start Time : 12 00 AM

  - **Monthly**. Select the day of the month on which the image task will run from the drop-down list.



Recurrence
Run this task : Monthly
Every : 1 date of every month
Start Date : 07/28/2011
Start Time : 12 00 AM

- **Start Date**. Select the date on which to start running the scheduled image task.
- **Start Time**. Specify the start time to run the scheduled image task.

5. When you are done configuring the new image task, click **Save**. You can then do the following via the toolbar:
   - Click **Delete** to delete the image task.
   - Click **Run Now** to run the image task immediately, otherwise the image task will run automatically at the next scheduled time.

Preparing a bootable USB device using the Create Live Image Media utility

The Recovery Disk Creation utility creates a bootable USB device that contains the files and software required to re-image your system.

Optionally, after the bootable USB device is created according to the following instructions, you can manually copy the backup image (TIB) file to the USB device as well. The TIB file MUST be located in a folder called called `Vertical\BackupImage` in order to be found by the re-imaging process.

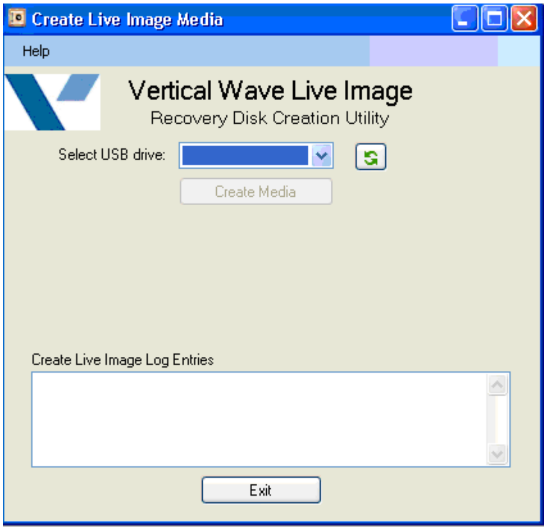
See “How Live Image works” on page 15-15 for details.

To create a bootable disk image using the Recovery Disk Creation utility

1. If you have not already done so, install the Recovery Disk Creation utility according to the information in “Installing Live Image” on page 15-17.
2. Launch the Recovery Disk Creation utility using any of the following methods:
   - From a command prompt, type CreateImageMedia.exe. Include the path to the folder where you installed the utility, or navigate to that folder before entering the command.
   - In Windows Explorer, double-click on CreateImageMedia.exe.
   - In Windows Explorer, right-click on CreateImageMedia.exe, and then choose **Run as administrator**.

   If you are not a member of the local system's Administrators group, a User Account Control (UAC) dialog opens, requesting a userid and password for a user with administrative privileges. If you are a member of the Administrators group, the UAC dialog requests confirmation that the application be allowed to make changes to this computer.

3 The Create Live Image Media dialog opens:

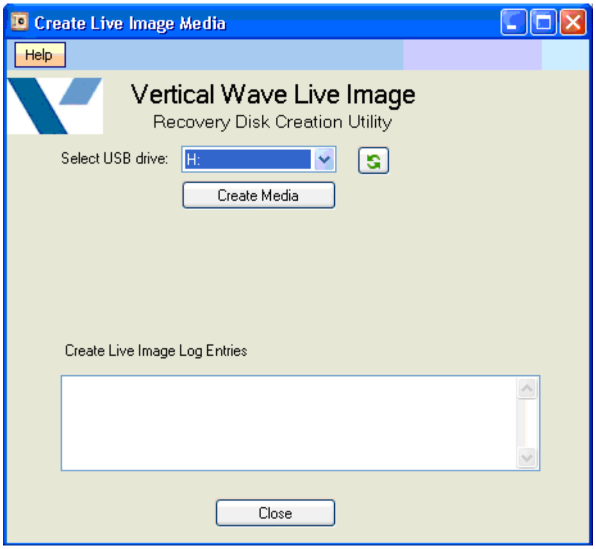


If no USB device is detected, the **Select USB drive** drop-down list is empty and the **Create Media** button is disabled.

4 If you have not already done so, insert a USB device (USB flash drive or USB enclosure) into the PC.

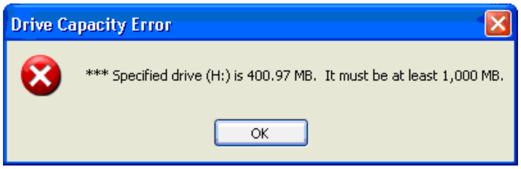
The **Select USB drive** drop-down list will refresh automatically when a USB device is inserted or removed. (You can also click the **Refresh** button.) Since the utility relies on the PC’s operating system to detect the device, it may take a few seconds before the drop-down list is refreshed.

Select the USB device to use.



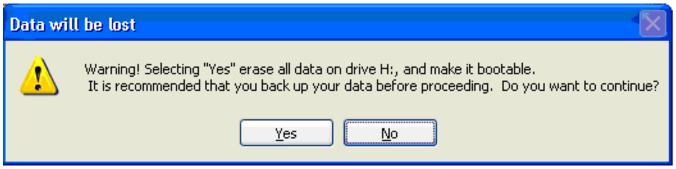
Select USB drive: H:

5 Click **Create Media**. If the selected device is too small, the following error message is displayed. If you see this error, replace the device with at least a 1GB drive and start over.



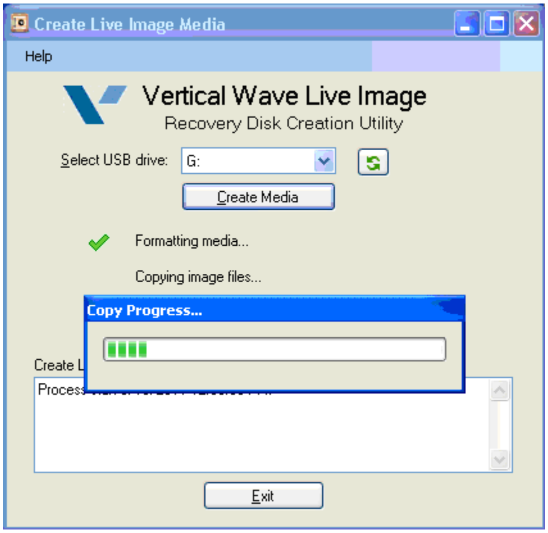
*** Specified drive (H:) is 400.97 MB. It must be at least 1,000 MB.

The following message opens, warning you that any data on the selected device will be destroyed. Click **Yes** to continue.



Warning! Selecting "Yes" erase all data on drive H:, and make it bootable.
It is recommended that you back up your data before proceeding. Do you want to continue?

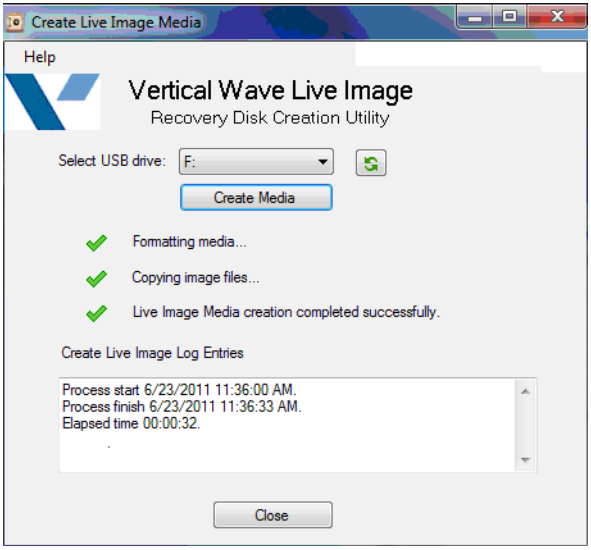
6 As the Recovery Disk Creation utility runs, a progress dialog opens, and progress indicators show the status.



✓ Formatting media...

Copying image files...

The following example shows a successful completion:



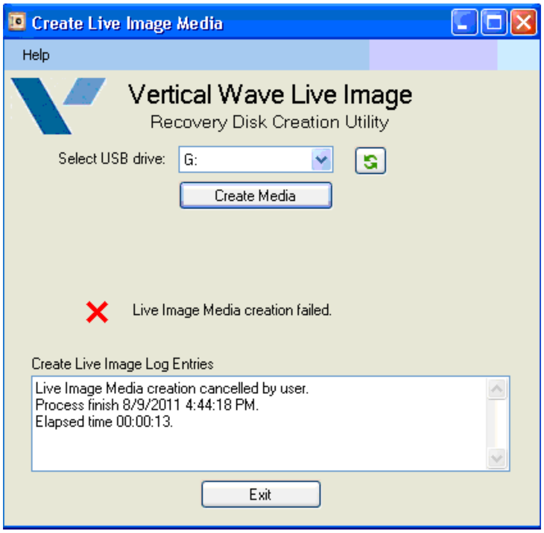
✓ Formatting media...

✓ Copying image files...

✓ Live Image Media creation completed successfully.

```
Process start 6/23/2011 11:36:00 AM.
Process finish 6/23/2011 11:36:33 AM.
Elapsed time 00:00:32.
```

The following example shows an unsuccessful completion:



Live Image Media creation failed.

```
Live Image Media creation cancelled by user.
Process finish 8/9/2011 4:44:18 PM.
Elapsed time 00:00:13.
```

If a processing failure occurs, review the information logged by the failing step in the **Create Live Image Log Entries** text box at the bottom of the dialog. This and more information will be logged to the application log file, located in the following location (relative to the folder where the utility was installed):

```
...\Logs\CreateImageMedia.log
```

7 Click **Close** to exit the Recovery Disk Creation utility.

8 Remove the bootable USB device. See “Re-imaging your system using a Live Image backup file” on page 15-30 for a detailed explanation of the risks of leaving a bootable USB device inserted in the Wave Server for any longer than necessary.

Re-imaging your system using a Live Image backup file

After creating a bootable USB device using the Create Live Image Media utility as described on page 15-25, make sure that the backup image (TIB file) to use resides in one of the following locations:

- On the USB device itself in a folder called `Vertical\BackupImage`.
- On a local hard drive or hard drive in a USB enclosure connected to the Wave Server, in a folder called `Vertical\BackupImage`. You cannot re-image your system from a TIB file on a network drive.

See “How Live Image works” on page 15-15 for important details about backup image files, including how the system searches for the backup image file to use for re-imaging.

Warning! **Do not leave *any bootable USB device* inserted in the Wave Server for extended periods of time, even if the device does not contain a Live Image backup file. Wave is equipped with self-correcting mechanisms, which may force a system reboot when certain thresholds are met. If a bootable USB device is encountered, either of the following may occur:**

- The boot sequence may stop after booting the USB device, preventing Wave from starting.
- The Wave Server maybe re-imaged, if the USB device contains a system recovery image or a valid Live Image backup file.

Note: This same behavior will occur if a system upgrade is invoked while a bootable USB device is inserted in the Wave Server.

To re-image your system using a Live Image backup file

1 Turn the Wave Server off. To do so, press and hold the red button on the front of the Server.

2 When you observe the following pattern on the LEDs on the front of the Wave Server, release the red button:

Status	LED1	LED2	LED3	LED4
Shutdown button press detected. System shutdown initiated.	**Green**	**Blinking red** / **solid green**	**Blinking green** / **blinking red**	**Blinking green**

System shutdown begins, and when complete, the Wave Server powers itself off.

3 Insert the bootable USB device directly into USB 2 port on the front of the Wave Server. Note the following:

- On a Wave IP 2500, the USB 2 port is the bottom USB port.
- On a Wave IP 500, the USB 2 port is the right-most USB port.

4 Restart the Wave Server. To do so, press the red button on the Wave Server faceplate.

5 After about 10 minutes, check the status LEDs on the front of the Wave Server. If system recovery was successful, the following alternating pattern repeats every 30 seconds:

Status	LED1	LED2	LED3	LED4
Normal firmware operation.	**Green**	**Blinking red** / **solid green**	**Blinking green**	**Blinking green**

6 After about 10 minutes, check the status LEDS on the front of the ISC:

- If system recovery was successful, the following alternating pattern repeats every 30 seconds:

System Status LEDs 1-4				Board LEDs 1-2	
off	**Green**	**Green**	**Green**	off	off
off	off	off	off	off	**Green**

Go to the next step.

- If system recovery was not successful, the following alternating pattern repeats every 15 seconds:

System Status LEDs 1-4				Board LEDs 1-2	
off	**Red**	**Red**	**Red**	off	off
off	off	off	off	**Red**	off

If system recovery was not successful, retry starting with step 1. If the problem persists, contact your Wave Technical Support representative.

7 Remove the bootable USB device.

8 Restart the Wave Server. To do so, use either the power switch at the back, or press the black reset button. Your Wave Server is now operational.

Part 2

Advanced Configuration and Administration

Chapter 16

PBX Feature Configuration

CHAPTER CONTENTS

Configuring authorization codes

Use the Authorization Codes applet to configure numeric passwords that allow users to place calls on phones and phone lines where call access is restricted.

Authorization codes can be used on analog, digital, and SIP phones. On digital phones, authorization codes can be used on both primary and secondary line appearances and outside lines. Refer to the *Wave Phone User Guide* for information about using authorization codes.

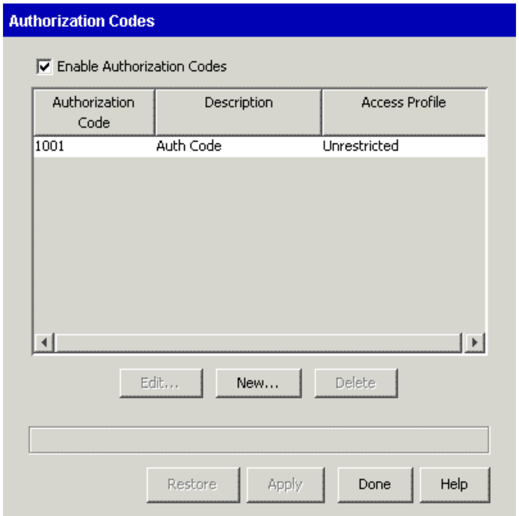
To add authorization codes

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Authorization Codes icon, located in the PBX Administration section.

The Authorization Codes applet starts.

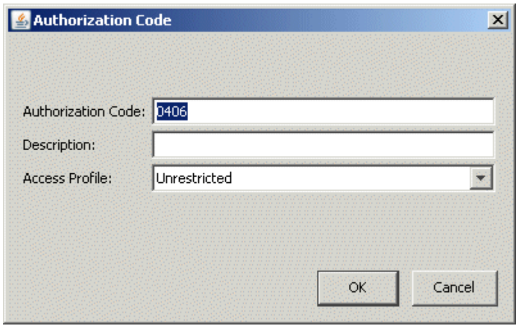


Authorization Codes

☑ Enable Authorization Codes

Authorization Code	Description	Access Profile
1001	Auth Code	Unrestricted

3 Click **New** to open the Authorization Code dialog.



Authorization Code

Authorization Code: 0406

Description:

Access Profile: Unrestricted

The Authorization Code field is automatically populated with a randomly selected unused 5-digit number. You may change this number to any 3- to 12-digit number.

4 Enter a **Description**.

5 Choose an Access Profile from the drop-down list.

The Access Profile determines what types of calls can be made on a Wave extension using this authorization code. The default is **Unrestricted** access.

6 Click **OK** to add the Authorization Code to the list.

7 Check the **Enable Authorization Codes** check box.

Authorization codes cannot be used until the Enable Authorization Codes check box is checked. When you are ready to enable authorization codes, check the Enable Authorization Codes check box.

8 Click **Apply** to save your changes.

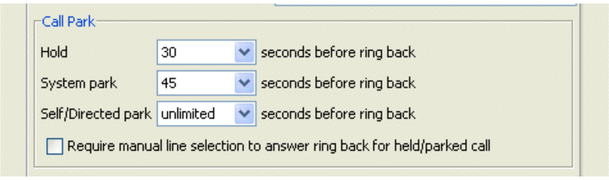
9 Click **Done** to return to the Management Console.

Configuring Call Park options

The Call Park feature places a call on an extension or in a system parking slot for retrieval from another phone.

1 In the General Settings applet, click the PBX Advanced tab.

2 In the Call Park group box, specify the following call park settings:



Call Park

Hold 30 seconds before ring back

System park 45 seconds before ring back

Self/Directed park unlimited seconds before ring back

□ Require manual line selection to answer ring back for held/parked call

- **Hold ___ seconds before ring back**. Select the number of seconds that Wave waits for a user to pick up a held call. If the call is not picked up within the specified time, Wave rings the extension from which the call was held.

  If you specify **unlimited** seconds, Wave does not ring back the extension.

- **System park ___ seconds before ring back**. Select the number of seconds that Wave waits for a user to pick up a parked call. If the call is not picked up within the specified time, Wave rings the extension from which the call was parked.

  If you specify **unlimited** seconds, Wave does not ring back the parking extension.

- **Self/Directed park ___ seconds before ring back**. Select the number of seconds that Wave waits for a user to pick up a self-parked (or directed-parked) call. If the call is not picked up within the specified time, Wave rings the extension from which the call was parked.

  If you specify **unlimited** seconds, Wave does not ring back the extension.

- **Require manual line selection to answer ring back for held/parked call**. This checkbox controls what happens when you pick up the handset of a phone that has a call on hold or a parked call on the primary line:

  - If checked, the phone provides dial tone when you pick up. To connect to the held/parked call, you must select its line manually.
  - If unchecked, picking up the phone connects you to the held/parked call on the primary line.

Configuring call pickup groups

You can configure call pickup groups—groups of extensions that can be answered by all the users in the group using the Group Pickup phone feature—and add extensions to them in the User/Group Management applet.

There are two methods to pick up a call in a pickup group:

- **Group**. Any group member can answer the ringing extension of any other group member. Members in this group can press the Group Pickup button on a digital phone or some SIP phone models, or dial ***74** to answer a call.
- **Extension**. A user specifies which ringing phone to answer. The user presses the Extn Pickup button on a digital phone (not supported on SIP phones), or dials ***75**+extension to pick up calls. Directed pickup works only for members of the same pickup group.

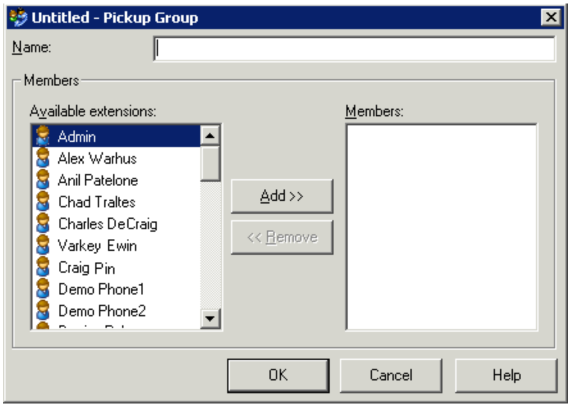
Note: An extension can belong to only one pickup group.

To create a pickup group

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the User/Group Management icon, located in the PBX Administration section of the Management Console.
3. Log on to the User/Group Management applet, which opens in a remote access window. Once you log on, the Users view opens. See “Accessing the User/Group Management applet” on page 2-15 for more about logging on to the User/Group Management applet.
4. Choose **File > New > Pickup Group**. The Pickup Group dialog opens.



5. Enter a **Name** for the Pickup Group.
6. Select the users you want and move them into the Members list by clicking **Add**. Hold down the CTRL key as you click to select multiple users. When assigning extensions to pickup groups, remember that an extension can belong to only one pickup group.
7. Click **OK**. The Pickup Groups that you have defined appear in the Pickup Groups view. Click its icon in the view bar of the User/Group Management applet to see and manage Pickup Groups.

Configuring Caller ID

Caller ID refers to the phone number and name that identify a caller. There are three types of Caller ID that you can configure in Wave:

- **External Caller ID** refers to the name and number that identifies the caller when a call is sent by Wave over an ISDN-PRI trunk to the central office. See page 16-6.
- **Internal Caller ID** refers to the name and number that identifies the caller on a station-to-station call that originates on the Wave Server or a PBX connected to the Wave Server. See page 16-9.
- **Inbound Caller ID** refers to the name and number that identifies the caller on a call received from an inbound call from an inbound trunk group, IP telephony source, or outside line. See page 16-9.

Configuring external Caller ID

External Caller ID refers to the name and number that identifies the caller when a call is sent by Wave over an ISDN-PRI trunk to the central office. External Caller ID can only be sent on an ISDN-PRI trunk. (Wave does not send Caller ID on analog trunks. If Caller ID is enabled on T-1 wink start or ground start trunks, the central office must be capable of receiving ANI/DNIS format.)

In order to send a name with the Caller ID information, the call must be placed on an ISDN trunk, the Send Caller Name option must be selected in the trunk configuration, and the far end has to accept the name. See “Configuring digital trunks and channels” on page 5-22 for information about enabling Caller ID on digital trunks.

When an internal extension initiates a call, its external Caller ID is determined by the settings configured in the General Settings and the User dialog, User \ External Caller ID tab. When a trunk initiates an outbound call (a tandem call) the external Caller ID is the same as the received Caller ID (or it is the trunk group name if no Caller ID is received).

By default, Wave sends no Caller ID to the trunks. Outbound trunk groups and IP telephony call destinations are the gatekeepers of external Caller ID. At this level Wave decides whether to send external Caller ID to the trunk and in what format.

To send Caller ID with outbound calls, you must perform the following tasks

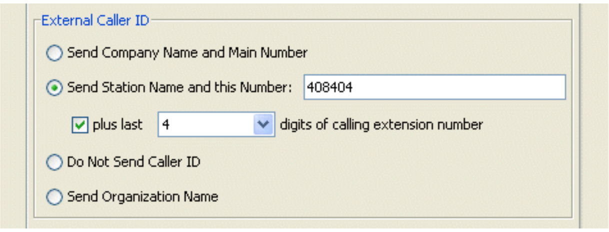
- Configure trunk-specific Caller ID settings (see “Configuring trunk-specific Caller ID settings” on page 16-10).
- Configure the system-wide Caller ID settings (see “Configuring system-wide Caller ID settings” on page 16-11).

By default, all internal extensions send the external Caller ID specified in the General Settings applet. For users with specific Caller ID requirements, configure the Caller ID settings in the User dialog to override the General Settings Caller ID format (see “Configuring user-specific Caller ID settings” on page 16-12).

Hierarchy of external Caller ID settings

External Caller ID can be applied at three different levels: system-wide, user-specific, and trunk-specific.

- **System-wide external Caller ID** is specified via the General Settings applet, PBX tab.


External Caller ID

○ Send Company Name and Main Number

● Send Station Name and this Number: 408404

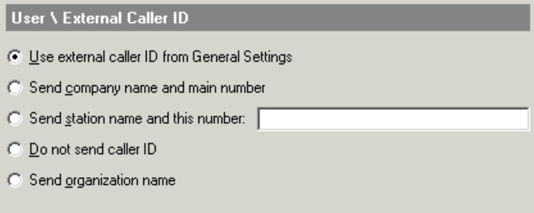
☑ plus last 4 digits of calling extension number

○ Do Not Send Caller ID

○ Send Organization Name

By default, system-wide external Caller ID is not sent.

- **User-specific external Caller ID** setting, if specified, overrides the system-wide setting. The user-specific external Caller ID setting is set for the user via the User/Group Management applet, User dialog \ External Caller ID tab.



User \ External Caller ID

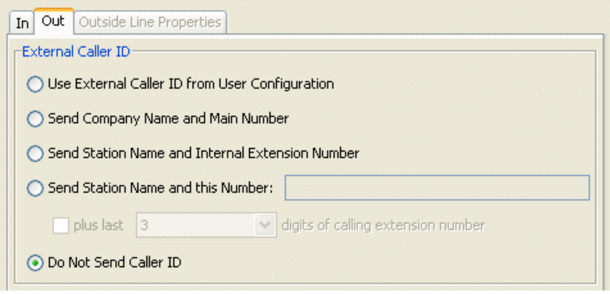
● Use external caller ID from General Settings
○ Send company name and main number
○ Send station name and this number:
○ Do not send caller ID
○ Send organization name

By default, external Caller ID at the user-specific level uses the system-wide setting.

- **Trunk-specific external Caller ID** setting, if specified, overrides the user-specific setting. By default, trunk-specific external Caller ID is not sent.

Trunk-specific external Caller ID can be set in two places:

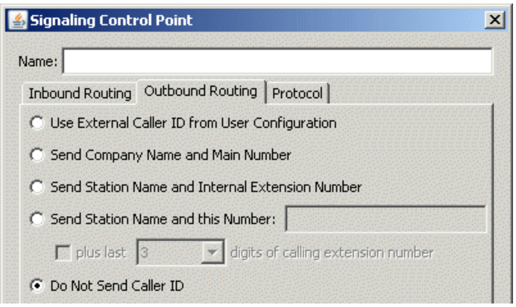
  - For outbound analog or digital trunks, external Caller ID is set via the Trunk Groups applet, Out tab.



External Caller ID

○ Use External Caller ID from User Configuration
○ Send Company Name and Main Number
○ Send Station Name and Internal Extension Number
○ Send Station Name and this Number:
□ plus last 3 digits of calling extension number
● Do Not Send Caller ID

  - For an outbound IP call destination, external Caller ID is set via the IP Telephony applet. (Click **Call Routing > Signaling Control Points**, edit the SCP, and then click the Outbound Routing tab.)



Name:

○ Use External Caller ID from User Configuration
○ Send Company Name and Main Number
○ Send Station Name and Internal Extension Number
○ Send Station Name and this Number:
□ plus last 3 digits of calling extension number
● Do Not Send Caller ID

For example, if at the system-wide level you choose to use the Company Name and Main Number, and at the user-specific level you choose to send no Caller ID, Caller ID will not be sent by calls made from that extension. However, if at the trunk-specific level you choose to send the Company Name and Main Number, then the Company Name and the Company Main Number are sent even though the user-specific Caller ID settings specified otherwise.

For more information, see:

- "Configuring system-wide Caller ID settings" on page 16-11.
- "Configuring user-specific Caller ID settings" on page 16-12.
- "Configuring trunk-specific Caller ID settings" on page 16-10.

Configuring internal Caller ID

Internal Caller ID refers to the name and number that identifies the caller on a station-to-station call that originates on the Wave Server or a PBX connected to the Wave Server. You do not need to configure internal Caller ID for extensions—it is always the Display Name and the extension number as specified in the User dialog.

Configuring inbound Caller ID

Inbound Caller ID refers to the name and number that identifies the caller on an inbound call received from an inbound trunk group, IP telephony source, or outside line. When a call arrives from a trunk (or IP telephony source), Wave may or may not receive Caller ID.

- If the Wave does receive Caller ID, this information is sent along with the call to its destination, whether it be internal or external.
- If Caller ID is not received, Wave assigns Caller ID information to the call depending on the call source:
  - **Inbound Trunk Group**. If the name is missing, the trunk group name (Digital, for example) is sent. If the number is missing, no number is sent.
  - **IP Telephony**. If the name is missing, "IP Telephony" is sent. No number is sent with an IP telephony call.

Configuring trunk-specific Caller ID settings

The trunk-specific Caller ID format determines whether Caller ID will be sent to the trunk and in what format. In the Trunk Groups and IP Telephony applets, you can configure the Caller ID values as they are supported by the trunks associated with the outbound trunk group or IP call destination. Configuring Caller ID on a particular outbound trunk group affects all the trunks and digital channels associated with the trunk group.

Caution! *Check your Service Confirmation Letter to determine whether Caller ID is supported on your trunks and in what format. Sending Caller ID to a trunk that does not support it might cause your calls to fail.*

To configure trunk-specific Caller ID settings

1 Specify the appropriate Caller ID settings for your application.

- **To specify Caller ID settings for an outbound trunk group**. In the Trunk Groups applet, edit the trunk group, and select the Out tab.
- **To specify Caller ID settings for an IP call destination**. In the IP Telephony applet, expand **Call Routing > Signaling Control Points**. Edit the call destination and click the Outbound Routing tab.

2 Select an external Caller ID setting:

- **Use External Caller ID from User Configuration**. For calls initiated from stations, sends external Caller ID as specified in the User dialog.
- **Send Company Name and Main Number**. Sends the Company Name and Company Main Number.
- **Send Station Name and Internal Extension Number**. For calls initiated from stations, sends the Display Name and extension number set in the User dialog.

  Use this setting for trunks connected to other PBXs.
- **Send Station Name and this Number**. For calls initiated from stations, sends the call source Display Name and the specified **Number**.

  Use this setting to provide the station name and phone number on outbound calls.

  Optionally, select the **plus last** check box to append the specified number of **digits of calling extension number** to the digits specified in the **Number** field.

  If the **plus last** check box is selected, the specified number of **digits of calling extension number** are appended to the digits specified in the **Number** field.

Use this setting to provide the station name and phone number on outbound calls.

Note: If this setting is your choice, it is generally recommended that you set this at the system-wide level in the General Settings applet.

- **Do Not Send Caller ID**. Sends no external Caller ID from this trunk group or IP call destination.

  Use this setting for trunks that do not support Caller ID, or for trunks where you want to block external Caller ID.

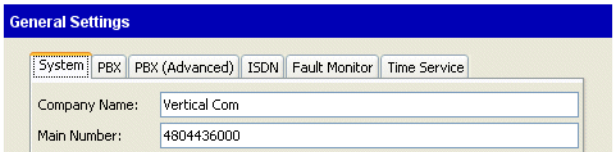
Configuring system-wide Caller ID settings

Configure the system-wide Caller ID settings for calls initiated by internal extensions in the General Settings applet. Remember that the external Caller ID is only sent to the central office if the trunk group is configured to send external Caller ID.

To configure system-wide Caller ID settings

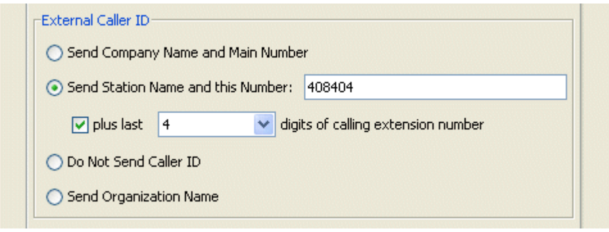
1 In the General Settings applet on the System tab, if you have not already done so enter the **Company Name** and Company **Main Number**.

Note: While **Company Name** can include up to 16 alphanumeric characters, Caller ID cannot send more than 15 characters over ISDN.


General Settings

Company Name: Vertical Com
Main Number: 4804436000

On the PBX tab, select a default External Caller ID setting for calls initiated by stations. Select one of the following options:

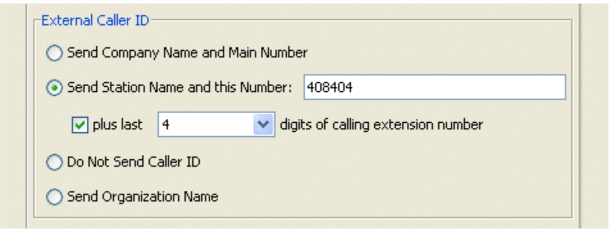

External Caller ID

○ Send Company Name and Main Number
● Send Station Name and this Number: 408404
☑ plus last 4 digits of calling extension number
○ Do Not Send Caller ID
○ Send Organization Name

- **Send Company Name and Main Number**. Sends the **Company Name** and Company **Main Number** as external Caller ID.

  Use this setting to provide some Caller ID information while keeping the actual calling extension number private.
- **Send Station Name and this Number**. Sends the Station Name (specified via the User/Group Management applet) followed by the digits entered in the adjacent field.

  If the check box is selected, the specified number of digits from the calling extension number are appended to the digits specified in the field.



External Caller ID

○ Send Company Name and Main Number

● Send Station Name and this Number: 408404

☑ plus last 4 digits of calling extension number

○ Do Not Send Caller ID

○ Send Organization Name

  For example, if you enter 4085227, and specify that the last 3 digits be added to the number, a call from extension 1234 will send the number 408-522-7234.

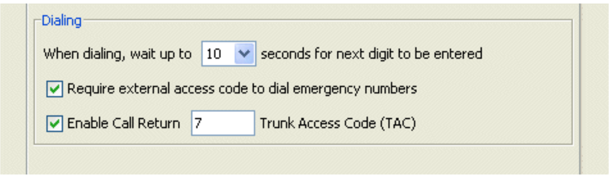
  Use this setting to provide the station name and phone number on outbound calls.
- **Do Not Send Caller ID**. Wave will not provide external Caller ID.
- **Send Organization Name**. *This option is not supported in this version.*

Configuring user-specific Caller ID settings

By default all users send the external Caller ID format specified in the General Settings applet. To override the system-wide Caller ID settings for a specific user, see “The User \ External Caller ID tab” on page 11-25.

Configuring dialing time-out

Configure the settings that determine how long Wave should wait after you finish dialing before placing the call.



Dialing

When dialing, wait up to 10 seconds for next digit to be entered

☑ Require external access code to dial emergency numbers

☑ Enable Call Return 7 Trunk Access Code (TAC)

Click

In the General Setting applet, PBX (Advanced) tab, in the Dialing section set **When dialing, wait up to ___ seconds for next digit to be entered**. This drop-down list sets the dialing timeout. If the specified time elapses before another digit is pressed, Wave will stop collecting digits and attempt to route the call based on the digits collected.

The dialing timeout is useful for dialing numbers of a length not expected by your dialing plan. For example, in North America, numbers are generally 7, 10, or 11 digits in length. If you are dialing an international number the length of the number will be longer than expected, or if you are dialing the local operator the number will be shorter. After you have finished dialing the number, Wave will wait the number of seconds specified in the drop-down list, and place the call as dialed.

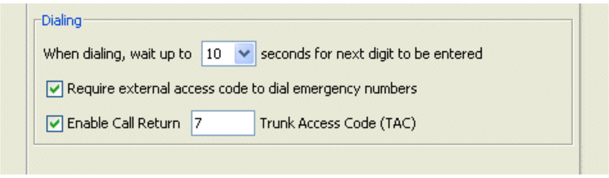
Requiring an access code for emergency number dialing

To help prevent accidental emergency calls, you can require users to dial an external access code before dialing an emergency number. This setting is disabled by default, since users may expect to simply dial the emergency number (for example “911”) to access emergency services.

Important! If you require an external access code to dial an emergency number, be sure that all users know about this requirement, and that they know the access code to use.

To require an external access code for emergency number dialing

1. In the General Settings applet, click the PBX (Advanced) tab.
2. Select the **Require external access code to dial emergency numbers** check box to enable this option. Deselect this checkbox if you want users to be able to dial an emergency number directly.



Dialing

When dialing, wait up to 10 seconds for next digit to be entered

☑ Require external access code to dial emergency numbers

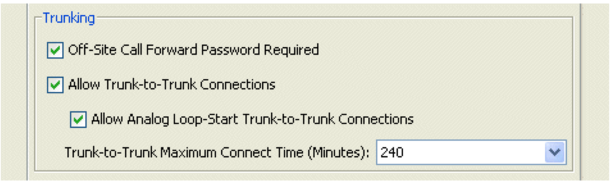
☑ Enable Call Return 7 Trunk Access Code (TAC)

You use the Outbound Routing applet to set up one or more emergency numbers. For details, see “Setting up emergency dialing” on page 9-43.

Configuring external call routing restrictions

Any time a call comes in to the Wave Server and is routed back out on another trunk (trunk-to-trunk), you must consider these external call routing restriction options. In this scenario a call is physically connected across two external trunks through the Wave Server.

Scenarios include off-site call forwarding, off-site transferring, and conferencing where two or more parties is an external phone number. These options can also affect your inbound call routing wherever you have an inbound call routed to an external destination.



Trunking

☑ Off-Site Call Forward Password Required

☑ Allow Trunk-to-Trunk Connections

☑ Allow Analog Loop-Start Trunk-to-Trunk Connections

Trunk-to-Trunk Maximum Connect Time (Minutes): 240

Click

You can configure the following options in the General Setting applet, PBX (Advanced) tab, in the Trunking group box:

- **Off-Site Call Forward Password Required**. Select this check box to require users to enter their voicemail passwords after specifying the external number when they forward their calls to an external phone number. (This option does not apply if a user is forwarding their phone to a Private Networking destination.)

Users without passwords can enter the password 111 when prompted to forward calls to an external number.

> **Note:** It is strongly suggested that you configure passwords for all users. Password security is crucial in preventing your company from being victimized by toll fraud, where unauthorized users gain privileged access to your telephone system and place outbound long distance or international calls that are then charged to you. In most cases, access is gained through unsecure, easy-to-guess passwords. By making your passwords more secure, you can dramatically increase the security of your Wave system against toll fraud. For more information, see Appendix Appendix A.

- **Allow Trunk-to-Trunk Connections**. To allow inbound calls to be routed to an external phone number, through forwarding, transferring, or inbound routing, you must select this check box. Also, select this check box to allow conferences where two or more parties are external phone numbers.
- **Allow Analog Loop-Start Trunk-to-Trunk Connections**. Select this check box to permit direct calls between analog loop-start trunks. Many connections of this type are left open, even after both parties hang up. If you select this check box, you can specify a maximum connect time in the Trunk-to-Trunk Maximum Connect Time field to ensure that the connection is closed after a specified amount of time.
- **Trunk-to-Trunk Maximum Connect Time (Minutes)**. This setting causes Wave to disconnect any trunk-to-trunk calls after the specified time limit. Setting this option helps avoid a situation where a trunk-to-trunk call is in a loop (for instance, both sides are busy) where neither side knows to terminate the call. Select Unlimited to prevent Wave from automatically terminating a trunk-to-trunk call.

Configuring Fax Redirect

The Fax Redirect feature allows you to automatically redirect incoming fax calls to the extension that has a fax machine. Without Fax Redirect, fax calls to an extension without a fax machine would not be received.

You can configure a fax redirect extension for the system, and you can override it for any auto attendant.

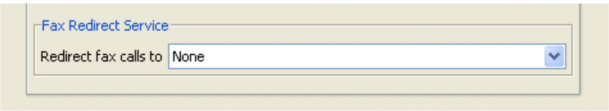
To configure Fax Redirect for the system

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Click the PBX tab of the General Settings applet.



Fax Redirect Service

Redirect fax calls to None

4 Under **Fax Redirect Service**, select the extension where faxes can be received from the **Redirect fax calls to** drop-down list.

Setting Fax Redirect for an auto attendant

For information on overriding the system fax redirect extension for calls to a particular auto attendant, see “Creating a new auto attendant” on page 13-3.

Setting up MeetMe Conference Rooms

The Wave MeetMe conference bridge makes it easy for internal and external callers to join a conference. Since a MeetMe conference room is simply an extension in your dial plan, all Wave call routing features (auto attendants, DID, Call Classifier, and so forth) work with conference rooms.

The MeetMe conference room feature expands Wave’s ad-hoc conferencing capability, but does not replace it. (Ad-hoc conferencing allows a user to call multiple parties and conference them together via Viewpoint or ViewPoint Mobile, or via the Conference / * Code feature on phones.)

MeetMe conferencing includes the following features:

- **Included with Wave**—no additional cost or licensing requirements, no installation steps.
- **Support for up to 18 conference rooms, with up to 24 attendees per conference**. The total number of simultaneous users in conference rooms is equal to the number of Conference Resources configured via Resource Management in the Global Administrator Management Console. Make sure to allocate enough conference resources to meet your needs.
- **Uses existing conference resources.**

- **Fully integrated with ViewPoint and ViewPoint Mobil**e. ViewPoint users can:
    - **View the conference rooms in the ViewPoint Extension pane**. Users can easily see if a conference room is in use by viewing the hook status icon for the conference room's extension—a conference room will be off-hook if at least one person is on the bridge.
    - **Call into a conference room** using any method currently supported in ViewPoint for calling an extension.
    - **Transfer a call to a conference room** using any method currently supported in ViewPoint or on the phone.
    - **View the attendee list** in the Calls pane > Parties tab.
    - **Mute or unmute any attendee** in a conference. The Calls pane > Parties tab shows whether an attendee is muted or unmuted. A user can unmute him or herself at any time.
    - **Disconnect an attendee**. Only a moderator can disconnect another moderator.
    - **Record the conference**.
    - **Add conference room extensions to the Favorites ta**b so they are easily accessible,
- **Set up a conference lobby**—You can create an auto attendant to handle calls to MeetMe conference rooms, and then provide the conference room extension to attendees so that they can join a specific conference.
- **Direct-dial conference rooms** are easy—You can assign a DID number to each MeetMe conference room so that external callers are connected directly to the associated conference room.
- **Moderator code**—You can optionally define a moderator access code for each conference room. If you define a moderator code for a conference room, callers are automatically joined into the conference room if the moderator has already logged in, or are held in a lobby (with music on hold playing) until a moderator arrives. A conference room can have one or more moderators—all attendees are conferenced together when any one of the moderators logs in; the conference ends and all attendees are disconnected when all of the moderators leave.
- **Access code**—You can optionally define an access code for each conference room that authorizes a caller to join the conference. If you define an access code, an attendee cannot join the conference until he or she enters the code correctly.
- You **control the maximum conference length** by setting an implicit timeout The default is 180 minutes.

- You can **add a conference room to the system call recording exclusion list**, so that calls involving the conference room are not included in system call recording.

  Note: Excluding a conference room from system call recording his does not prevent any individual user from recording the conference.

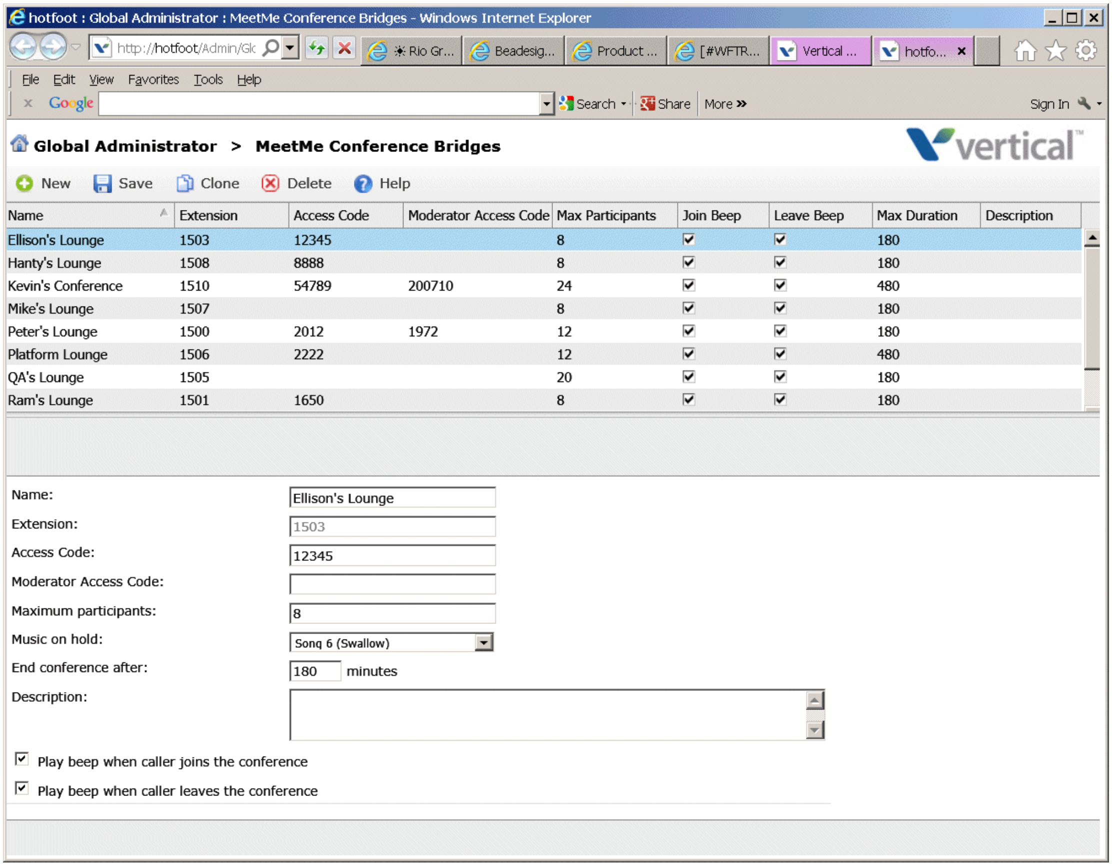
Allocating system resources for MeetMe conferencing

MeetMe conferencing uses the same All Conferencing resources as does ad-hoc conferencing. Conference resources will be made available for MeetMe and ad-hoc conference requests on a first-come, first-served basis—all conferences are treated equally when requesting available conference resources, so be sure to allocate enough conference resources for your specific needs.

To create a new MeetMe conference room

1 In the Global Administrator Management Console, click **MeetMe Conference**, located in the General Administration section.

2 The MeetMe Conference Bridges view opens, showing any conference rooms that have been created so far. The details for the selected conference room are displayed at the bottom of the view.


hotfoot : Global Administrator : MeetMe Conference Bridges - Windows Internet Explorer
http://hotfoot/Admin/Gk
File Edit View Favorites Tools Help
Google
Search
Share
More »
Sign In
vertical
New
Save
Clone
Delete
Help

Global Administrator > MeetMe Conference Bridges

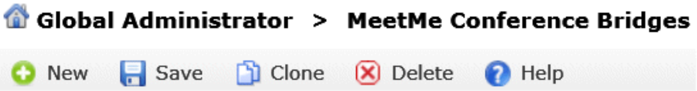
Name	Extension	Access Code	Moderator Access Code	Max Participants	Join Beep	Leave Beep	Max Duration	Description
Ellison's Lounge	1503	12345		8	☑	☑	180	
Hanty's Lounge	1508	8888		8	☑	☑	180	
Kevin's Conference	1510	54789	200710	24	☑	☑	480	
Mike's Lounge	1507			8	☑	☑	180	
Peter's Lounge	1500	2012	1972	12	☑	☑	180	
Platform Lounge	1506	2222		12	☑	☑	480	
QA's Lounge	1505			20	☑	☑	180	
Ram's Lounge	1501	1650		8	☑	☑	180	

Name:	Ellison's Lounge
Extension:	1503
Access Code:	12345
Moderator Access Code:	
Maximum participants:	8
Music on hold:	Song 6 (Swallow)
End conference after:	180 minutes
Description:	

☑ Play beep when caller joins the conference

☑ Play beep when caller leaves the conference

3 Click **New** on the toolbar at the top of the view.

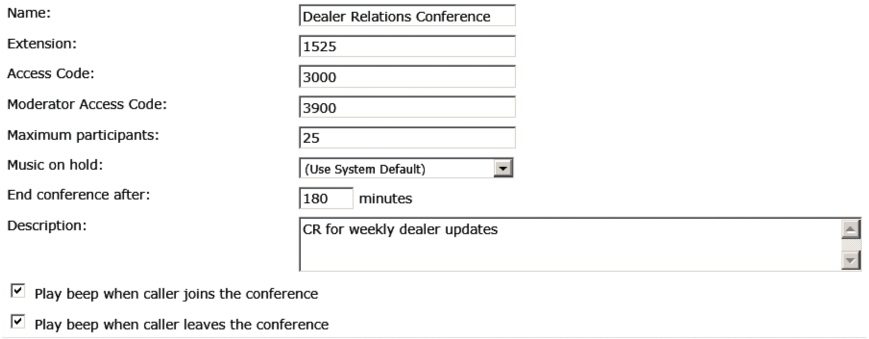


4 Enter the following information:

- **Name**. Each conference room name must be unique, and cannot be the same as any other entry that appears in the ViewPoint Extensions pane (user name, hunt group name, auto attendant name, or queue name).
- **Extension**. Start typing a valid Wave extension, then select the extension from the list of matching extensions.
- **Access Code**. Optionally, enter a 1-10 digit access code that attendees must supply to enter the conference room.
- **Moderator Access Code**. Optionally, enter a 1-10 digit access code that moderators must supply to start and end a conference.
- **Maximum participants**. Enter a value from 3 to 24.
- **Music on hold**. Select the music-on-hold source to use from the drop-down list.

  Select **Disabled** if you do not want attendees to hear music on hold while they are waiting to enter the conference room, or while they are muted.
- **End conference after**. Enter the maximum length of a conference in minutes. Three minutes before this time limit elapses, attendees will hear a prompt that the conference will be ending soon. The conference ends automatically when the time limit is elapses.

  You can specify maximum conference length from 1 to 9999 minutes, with a default value of 180 minutes.
- **Description**. Enter a description of up to 250 characters.
- **Beep settings**. Optionally, select a check box to play a beep when a caller joins or leaves the conference.



Name:	Dealer Relations Conference
Extension:	1525
Access Code:	3000
Moderator Access Code:	3900
Maximum participants:	25
Music on hold:	(Use System Default)
End conference after:	180 minutes
Description:	CR for weekly dealer updates

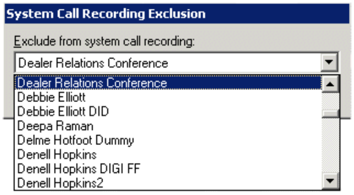
☑ Play beep when caller joins the conference

☑ Play beep when caller leaves the conference

5 Click **Save** on the toolbar to save the new conference room.

To exclude a MeetMe conference room from system call recording

1. In the Global Administrator Management Console, click **User/Group Management**, located in the PBX Administration section.
2. Choose **Tools > System Settings**. The System Settings dialog opens.
3. Expand **Recording / System Call Recording** in the left pane.
4. In the right pane, click **Add**.
5. In the System Call Recording Exclusion dialog, select the conference room to exclude from the drop-down list, and then click **OK**.



System Call Recording Exclusion

Exclude from system call recording: Dealer Relations Conference

6. Click **OK** to save your changes.

Configuring Music On Hold

The system-wide music on hold source identifies the music that all callers on hold hear unless a user, auto attendant, or queue is configured to use a different source (see “Customizing music on hold” on page 16-25.)

This section describes the following:

- **Configuring a system port for music on hold**. This step is required before you can select a specific WAV file to play to callers on hold, either (one of the options described later in this section). See page 16-21.
- **Enabling system-wide music on hold**. See page 16-22.

For information about music on hold for IP calls, see Configuring music on hold for IP calls“Configuring music on hold for IP calls” on page 6-52.

To configure a system port for music on hold

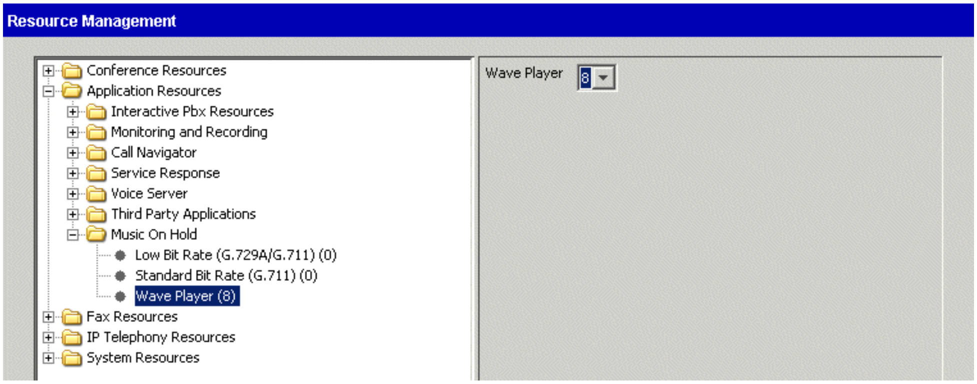
Click

1. If necessary, click the Administration tab of the Management Console.
2. Click the Resource Management icon, located in the PBX Administration section

3 Expand the Application Resources folder.

4 Expand the Music On Hold folder, and then select **Wave Player**.

5 Select a port from the **Wave Player** drop-down list.



Resource Management

- ⊞ Conference Resources
- ⊟ Application Resources
  - ⊞ Interactive Pbx Resources
  - ⊞ Monitoring and Recording
  - ⊞ Call Navigator
  - ⊞ Service Response
  - ⊞ Voice Server
  - ⊞ Third Party Applications
  - ⊟ Music On Hold
    - Low Bit Rate (G.729A/G.711) (0)
    - Standard Bit Rate (G.711) (0)
    - Wave Player (8)
- ⊞ Fax Resources
- ⊞ IP Telephony Resources
- ⊞ System Resources

Wave Player 8

6 Click **Apply** to save your changes, and click **Done** to close the Resource Management applet.

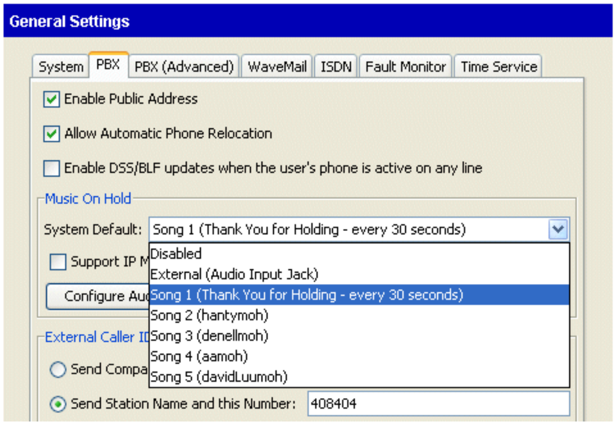
To enable system-wide music on hold

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the PBX tab. In the **Music On Hold** section, specify the music-on-hold source to use as the **System Default** from the drop-down list:



General Settings

☑ Enable Public Address

☑ Allow Automatic Phone Relocation

□ Enable DSS/BLF updates when the user's phone is active on any line

Music On Hold

System Default: Song 1 (Thank You for Holding - every 30 seconds)

- Disabled
- External (Audio Input Jack)
- Song 1 (Thank You for Holding - every 30 seconds)
- Song 2 (hantymoh)
- Song 3 (denellmoh)
- Song 4 (aamoh)
- Song 5 (davidLuumoh)

□ Support IP M

External Caller II

○ Send Compa

● Send Station Name and this Number: 408404

Select one of the following options:

- **Disabled.** No default music-on-hold source is specified. This setting does not affect a music-on-hold source specified for an individual user, auto attendant or Contact Center queue.

  Hint: It is highly recommended that you specify a default music-on-hold source so that a caller who reaches a user, auto attendant, or queue with no music-on-hold source specified does not hear extended ringing or silence, which may result in a hang-up.

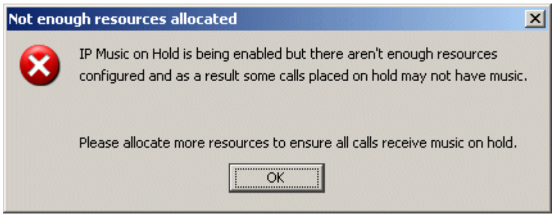
- **External (Audio Input Jack)**. Hold music is played from an external device, typically a CD player, radio, or specialized music-on-hold device. For more about using external music-on-hold devices with Wave, see “Music-on-hold systems” in Appendix B in the *Wave Server Hardware Reference Guide*.

  Note: Wave plays whatever is on the specified channel and does not monitor the channel. If the music device stops, callers on hold hear nothing.

- **Song n (<song title>)**. Select the WAV file to play to callers on hold. You cannot select a specific WAV file here until you configure a system port for music on hold (described above). You identify the WAV files that are listed here via the Configure Audio Sources dialog, described in step 5.

4 To play hold music to calls on SIP phones or SIP trunks, select the **Support IP Music On Hold** checkbox.

Important! If you see the following message, you need to exit the General Settings applet, allocate additional Music on Hold resources (either Low Bit Rate (G.729A/G.711) or Standard Bit Rate (G.711) resources) via the Resource Management applet, and then restart the General Settings applet.

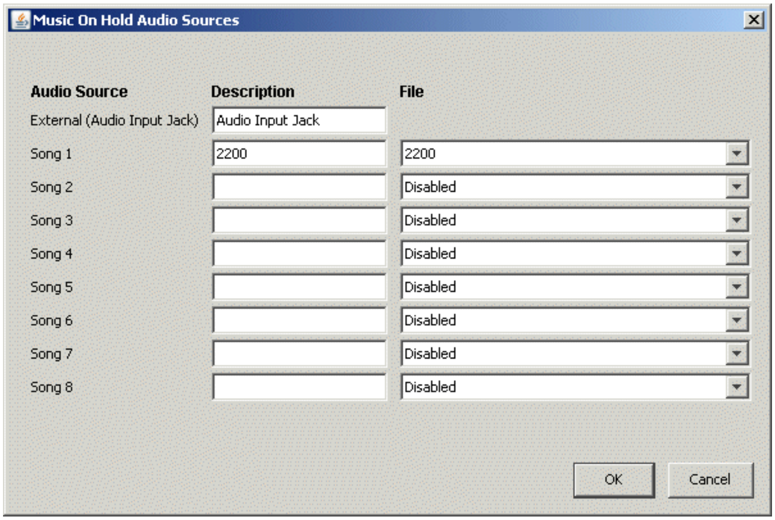


Not enough resources allocated

IP Music on Hold is being enabled but there aren't enough resources configured and as a result some calls placed on hold may not have music.

Please allocate more resources to ensure all calls receive music on hold.

5 Click **Configure Audio Sources** to open the Music On Hold Audio Sources dialog:.



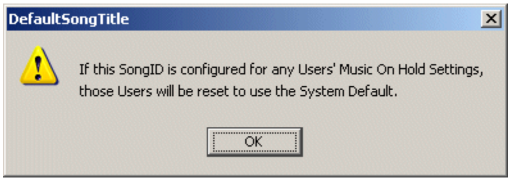
Music On Hold Audio Sources

Audio Source	Description	File
External (Audio Input Jack)	Audio Input Jack	
Song 1	2200	2200
Song 2		Disabled
Song 3		Disabled
Song 4		Disabled
Song 5		Disabled
Song 6		Disabled
Song 7		Disabled
Song 8		Disabled

You use this dialog to identify the external and internal audio sources displayed in the **System Default** drop-down list (described above), and also in the music on hold source drop-down lists available when you edit a user, user template, auto attendant, or Contact Center queue.

- **External (Audio Input Jack)**. Enter a descriptive label for the external music on hold device if you are using one, for example “FM Top 40 radio”.
- **Song 1 - Song 8**. You can make up to 8 WAV files available for use in various music-on-hold scenarios. For each entry:
  - Select the song title or filename from the **File** drop-down list.
  - Enter a **Description** that will help users understand how various WAV files can be used, for example “After-hours main MOH”. If you do not enter a **Description**, the **File** name is used.

  To take a song out of use, select **Disabled** from the drop-down list. If you disable a song the following warning message is displayed, indicating that some users’ music-on-hold settings may be reset.



DefaultSongTitle

If this SongID is configured for any Users' Music On Hold Settings, those Users will be reset to use the System Default.

6 For more about creating and placing custom audio files for hold music, see “Customizing music on hold” on page 16-25Click **Apply** or **Done** to save your changes. Your music on hold settings take effect immediately. However, calls currently on hold without music will remain without music. If you switch from a WAV file to an External hold music source, SIP calls currently on hold will continue to hear the WAV file.

Customizing music on hold

Each user, auto attendant, and Contact Center queue can have individualized hold music that is different from the default system hold music. See the following:

- **User**. See “Setting the user’s hold music” on page 11-90
- **User template**. See “The Audio \ Hold Music, Voice Title, and Disk Usage tabs” on page 11-89
- **Auto attendant**. See “Setting up an auto attendant’s hold music and greetings” on page 13-20
- **Contact Center queue**. See “Setting up hold music” in Chapter 2 in the *Wave Contact Center Administrator Guide*.

Important! You can select a specific WAV file to play to callers on hold in any of these scenarios. Before you can do so, you must first set up a system port for music on hold, as described in “Configuring Music On Hold” on page 16-21.

Using custom audio files for system hold music

You can use your own audio files for system hold music. To do so, you must convert each audio file to the format required by Wave, and then place the files in the correct location on the Wave Server. Custom audio files must be in 8-bit mu-law 8000 Hz mono WAV format—system hold music will not play back if you use a different file format.

To create audio files for music on hold

1 Start with a audio file (WAV, MP3, and so forth) of your choice.

2 Launch an audio conversion tool. A recommended one is SmartSoft’s Smart WAV converter, available at http://www.smartwavconverter.com. (You will need the pro version.)

3 Convert your audio file to 8-bit mu-law 8000 Hz mono WAV file format and save it.

To place the music on hold audio files in the correct locations

1 Copy the converted WAV file to the following location on the Wave Server:

```
C:\Inetpub\ftproot\Private\Options\Music
```

2 If you have SIP phone users or IP trunks, copy the converted WAV file to the following location:

```
C:\Inetpub\ftproot\Private\Options\IpMOHMusic
```

Enabling Public Address

The Public Address feature requires third-party hardware for amplification on an analog-only Wave system. If you have digital phones, the speakers on the phones act as a public address system and announcements are sent to digital phone speakers as well as the overhead public address system.

To enable the public address system

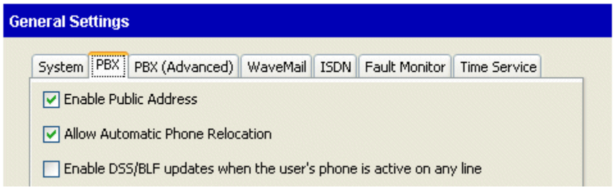
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the PBX tab.

4 Select the **Enable Public Address** check box.



General Settings

☑ Enable Public Address

☑ Allow Automatic Phone Relocation

☐ Enable DSS/BLF updates when the user's phone is active on any line

Once Public Address is enabled, users can make announcements over the public address system and digital phone speakers by pressing the System Page button on digital phones, or dialing ***11**. For more information about the System Page feature, see “Page feature” on page 10-27.

Enabling automatic phone relocation

When automatic phone relocation is enabled on the Wave Server, a previously-working digital phone will be recognized after it has been unplugged and moved to a new location, for example if a user switches offices. You do not need to manually reassign the phone's extension or reprogram feature buttons after a move.

Automatic phone relocation supports two methods of phone relocation, depending on the digital phone type:

- **Auto recognition** is supported only on Comdial digital phones (Edge100, 700, 80xx, and 83xx).

  Comdial digital phones store the extension assigned when the phone last came into service. When a previously-working Comdial digital phone is plugged in at the new location, the user is asked if he or she wishes to retain the extension assigned to the phone.

  - If the user responds YES, all phone-specific information—programmed feature buttons, speed dial numbers, and so forth—is retained at the new location.
  - If the user responds NO (or if the user lets the question time out after about 2 minutes), ***98** must be used for automatic phone relocation, as described below.

- **Relocation Feature Code *98** is supported on *all* digital phones, including those listed above. Dialing ***98** + an extension on a digital phone assigns that extension to the phone. The extension to be assigned cannot currently be in service.

  A user can use ***98** to either physically move his or her digital phone to a new location, or to swap a phone with another user. For example, Joe (x201) is moving into Frank's (x205) old office. They both have the same digital phone model. Joe unplugs his phone (so x201 is no longer in service) and leaves it in his old office. He then goes to his new office and dials ***98 201** on Frank’s old phone. Frank's phone is configured with Joe's extension with all of Joe's feature buttons, call history, and other phone information automatically relocated from his old phone.

  The phone must be operable before the user can dial ***98** from it. This means that one of the following must be true:

  - The new slot and port where the phone is relocated to must already be preprogrammed as a similar phone model (via the **slot/port** and **Telephone type** fields on the User tab of the User dialog).

    In this case, the phone will come into service as the extension of whichever user is programmed at that slot/port, and then ***98** can be dialed to reassign the new extension to this slot/port. The slot/port of the user that was previously programmed at that location will be cleared, but the user itself will not be deleted.

  - There must be one or more users (extensions) defined in the Wave database with a similar **Telephone type** but with no **slot/port** assigned.

    In this case, when a phone is plugged into a slot/port that is not associated with any extension and available unassigned extensions exist in the database, the Auto Configuration feature is invoked and “BEGIN” is displayed on the phone’s LED screen to allow an available extension to be selected. Once an available extension is selected the phone will come into service as that extension. Then ***98** can be dialed to assign the relocating user’s extension to this phone. Note that the relocating user’s extension is not offered during Auto Configuration because in the Wave database it is still associated with the slot/port at its old location.

  If neither of these configuration scenarios is true, the phone’s LED display will show the slot and port the phone is plugged into, and a status of “Unassigned”. Until you resolve one of the scenarios, the phone will never come into service and you will not be able to use ***98**.

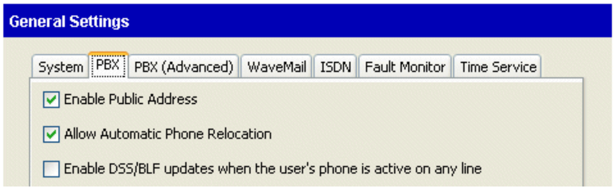
To configure automatic phone relocation

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 In the PBX tab of the General Settings applet, select the **Allow Automatic Phone Relocation** check box.



☑ Enable Public Address

☑ Allow Automatic Phone Relocation

□ Enable DSS/BLF updates when the user's phone is active on any line

4 Click **Apply** to save your changes.

5 Click **Done** to return to the Management Console.

Enabling DSS/BLF updates when the user's phone is active on any line

A Direct Station Select/Busy Lamp Field (DSS/BLF) feature button on a digital phone monitors the state of a specific extension, and provides a quick way for a user to place or transfer a call to that extension. A DSS/BLF feature button can be in one of the following states:

- A solid red LED next to a DSS/BLF button indicates that the extension is in use.
- A flickering red LED indicates the extension is ringing.
- A blinking LED indicates that the extension has a call on hold, or the extension is in Do Not Disturb mode.

By default, the DSS/BLF feature button only reflects the state of the assigned extension's primary line. When you perform the steps described below, a DSS/BLF feature button on a user's digital phone will reflect the assigned extension's state for any line, not just the extension's primary line. For example, if the user at extension 201 is busy on an Outside Line or on a line appearance, another user with a DSS/BLF feature button assigned to extension 201 will see that the user is busy on a call.

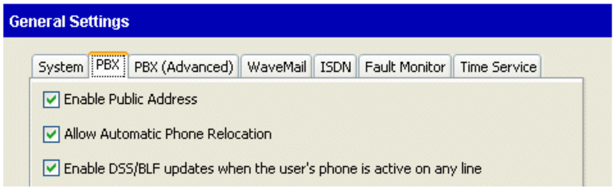
To enable DSS/BLF updates when a user’s phone is active on any line

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 In the PBX tab of the General Settings applet, select the **Enable DSS/BLF updates when the user’s phone is active on any line** check box.



☑ Enable Public Address

☑ Allow Automatic Phone Relocation

☑ Enable DSS/BLF updates when the user's phone is active on any line

4 Click **Apply** to save your changes.

5 Click **Done** to return to the Management Console.

Note: This option is enabled or disabled on a global basis for all users.

Enabling call return for external calls

This option allows a user to automatically call back the last inbound external call via the ***69** phone command or a phone feature button configured for Call Return. If this option is not enabled, users cannot automatically call back external calls. The Trunk Access Code (TAC) that you specify according to the following steps is prepended to the phone number of most recent inbound external call before the call is returned.

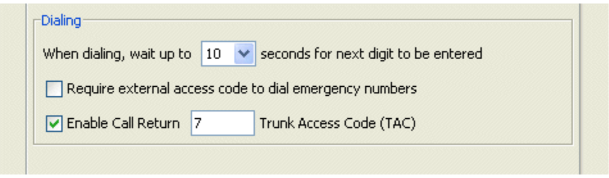
To enable call return for external calls

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 In the PBX (Advanced tab) of the General Settings applet, in the Dialing section select the **Enable Call Return ___ Trunk Access Code (TAC)** check box.



Dialing

When dialing, wait up to 10 seconds for next digit to be entered

☐ Require external access code to dial emergency numbers

☑ Enable Call Return 7 Trunk Access Code (TAC)

4 Enter the trunk or external access code required to make an external call, typically 9.

5 Click **Apply** to save your changes.

6 Click **Done** to return to the Management Console.

Configuring Night Answer

The Night Answer feature enables you to manually place the Wave Server into a mode where inbound calls are redirected to predetermined destinations. You can configure any extension or external phone number as the destination.

To put the Wave Server in or out of Night Answer mode

- On digital phones, configure a Night Answer button to activate and deactivate Night Answer. When Night Answer is active, the LED flashes red. When Night Answer is not active, the LED is dark.
- On phones without a Night Answer button, dial ***85** to activate Night Answer and ***86** to deactivate Night Answer.

To configure Night Answer

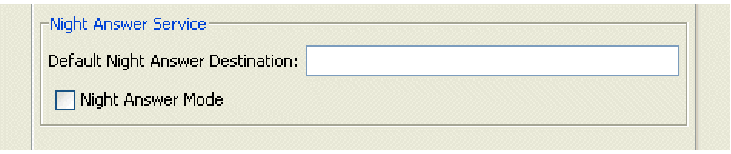
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 In the PBX tab of the General Settings applet, select the **Night Answer Mode** check box.

4 Enter a destination in the **Default Night Answer Destination** field.



Night Answer Service

Default Night Answer Destination:

□ Night Answer Mode

5 Edit your inbound trunk groups' Inbound Routing Tables to specify the correct night answer mode in the Night Answer Mode field.

- If you are configuring your incoming T-1 or analog trunks for Night Answer, open the Trunk Groups applet and edit your Inbound Routing Tables.
- If you are configuring your incoming IP Telephony calls for Night Answer, open the IP Telephony applet, select Default Inbound Routing from the Call Routing folder, and click the **Edit Inbound Routing Table** button.

The available Night Answer Modes are as follows:

- **Not Used**. Disables the Night Answer Mode for this trunk group
- **Use System Default**. Uses the Default Night Answer Destination specified in the General Settings applet

  Note: Select an Access Profile for Tandem Calls in the Inbound Trunk Group dialog and enable Allow Trunk-to-Trunk Connections in the General Settings (PBX (Advanced) tab) if the Default Night Answer Destination you specified in General Settings is an off-premise call and not routed using the Global Access outbound routing rules.

- **User Defined**. Uses the destination that you enter in the Night Answer Destination field in the Inbound Routing Table and it overrides the system default specified in the General Settings applet

  Note: Select an Access Profile for Tandem Calls in the Inbound Trunk Group dialog and enable Allow Trunk-to-Trunk Connections in the General Settings (PBX (Advanced) tab) if the Night Answer Destination you specified is an off-premise call and not routed using the Global Access outbound routing rules.

Note: The night answer mode configuration is not allowed for the Modem trunk group.

6 If you want to configure digital phones with a Night Answer button, change the configuration of the those phones in the User Configuration (Templates) applet.

Configuring System Speed Dial

Use the System Speed Dial applet to assign 1-3 digit speed dial numbers to phone numbers that your organization uses frequently.

System speed dial numbers can be used on all phones (digital phones can use the pre-programmed System Speed Dial button while analog and IP phones can use the *89 code). See the *Wave Phone User Guide* for information about using system speed dial numbers from the phone.

See the following sections for more about the System Speed Dial feature:

- Adding speed dial numbers. See page 16-33.
- Setting the System Speed Dial password. See page 16-35.
- Adding speed dial numbers using the phone. See page 16-35.

Adding speed dial numbers

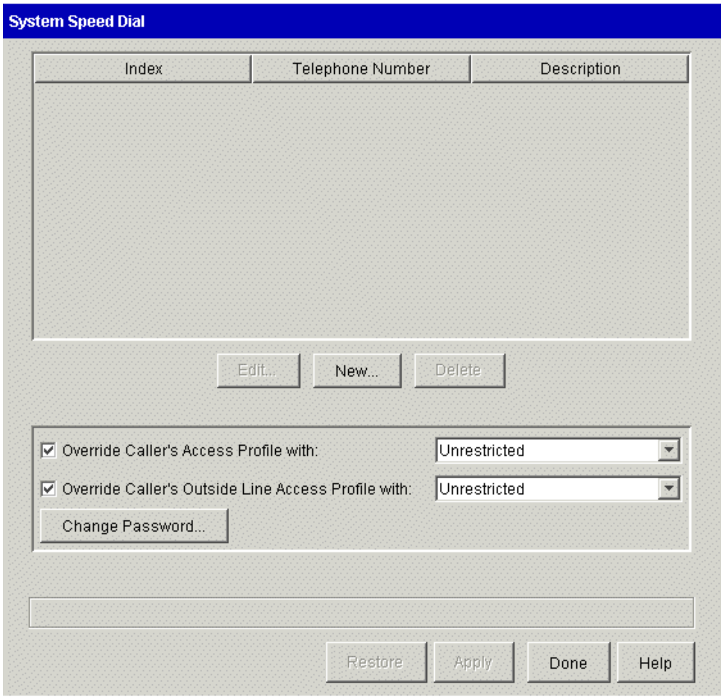
To add speed dial numbers in the System Speed Dial applet

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the System Speed Dial icon, located in the PBX Administration section.

3 Click **New.**

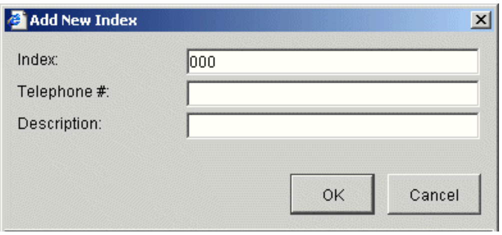

System Speed Dial

Index	Telephone Number	Description

☑ Override Caller's Access Profile with: Unrestricted

☑ Override Caller's Outside Line Access Profile with: Unrestricted

4 Click **New** to open the Add New Index dialog.


Add New Index

Index: 000

Telephone #:

Description:

5 Enter the speed dial number in the **Index** field.

The **Index** field is automatically filled in with the next available index number. You can enter any number in the range `000-999`.

6 Enter the phone number in the **Telephone #** field.

A phone number can be any digit sequence up to 32 digits in length. Be sure to include the external access code if necessary.

Note: Phone numbers for external calls must include the first digit defined in the First Digit Table applet for external dialing access. These external speed dial numbers can be dialed using primary lines, secondary line appearances, and outside lines.

7 Enter a **Description** for the speed dial number. The description can be any character sequence up to 20 characters in length.

8 Click **OK** to close the Add New Index dialog.

9 Click **Apply** to save your changes.

10 Click **Done** to return to the Management Console.

Setting the System Speed Dial password

The System Speed Dial password is used when you add a system speed dial number using the phone as described in “Adding speed dial numbers using the phone” on page 16-36. By default, the system speed dial password is set to 11111.

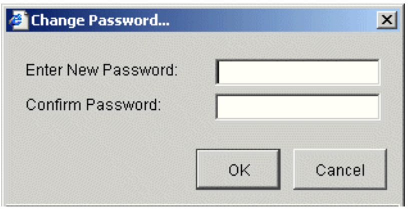
To set the System Speed Dial password

1 If necessary, click the Administration tab of the Management Console.

Click ☎

2 Click the System Speed Dial icon, located in the PBX Administration section.

3 Click **Change Password**.


Change Password...

Enter New Password:

Confirm Password:

4 Enter a five-digit password in the **Enter New Password** field.

5 Enter the password again in the **Confirm Password** field.

6 Click **OK**.

7 Click **Apply** to save your changes.

8 Click **Done** to return to the Management Console.

Adding speed dial numbers using the phone

To add a speed dial number using the phone

1 From any Wave phone, dial ***88**.

2 Enter the following in sequence:

- **5-digit System Speed Dial password**. The default password is `11111`.
- **3-digit speed dial index number**. You can enter any number in the range `000-999`.
- **Phone number**. A phone number can be any digit sequence up to 32 digits in length. Include the trunk access code (for example, 9) for external calls.

3 Press # to save the number.

For example, using the following format:

```
*88 + [password] + [index] + [phone number] + #
```

You might enter:

```
*88 12345 123 914085551212 #
```

This example creates the system speed dial number “123” that automatically dials 9 for external access and then the number 1-408-555-1212.

- If the password you entered is correct, Wave responds with two beeps indicating that the speed dial number was created. The new number overwrites any number previously stored at that index.
- If the password is incorrect, Wave responds with a fast-busy tone.

A default description is created in Wave’s System Speed Dial table based on the extension number from which the speed dial number was added. After adding a speed dial number using the phone, you can open the System Speed Dial applet to view and edit the default description. See “Adding speed dial numbers” on page 16-33.

Overriding access profiles when using System Speed Dial

By default, Wave does not override an access profile assigned to a line appearance if its extension does not have permission in its access profile to dial long distance numbers. For example, if an extension's phone line appearances have Local Only access profiles assigned to them, a user at that extension cannot use any system speed dial numbers that correspond to long distance phone numbers.

If you want users with restrictive access profiles to be able to use system speed dial numbers that require a higher level access profile, you must override the user's access profile in the System Speed Dial applet.

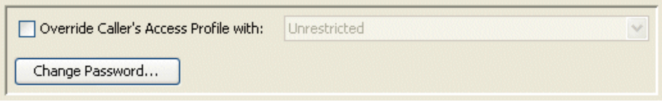
To override user access profiles when using System Speed Dial

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the System Speed Dial icon, located in the PBX Administration section.

3 Select the **Override Caller's Access Profile** checkbox to override a line appearance access profile with the specified access profile when a user dials any system speed dial number on a Wave extension. Select the access profile to use from the drop-down list.



□ Override Caller's Access Profile with: Unrestricted

Note: Access profiles for line appearances are configured in the Outbound Routing applet; see "Configuring specific access profiles" on page 9-14.

4 Click **Apply** to save your change.

5 Click **Done** to return to the Management Console.

Configuring virtual extensions

Configure virtual extensions for users who do not need a physical phone, but require an office extension. These users might be employees who work on the road with a cell phone, but who need to have an office extension listed in the Voicemail Names Directory (see Chapter 13, Configuring Auto Attendants).

You can configure up to 1024 virtual extensions.

If you configured SIP stations on a system running Wave ISM 1.5 SP2 or earlier. The maximum number of virtual extensions was increased from 500 to 1024 in Wave ISM 1.5 SP2. SIP station IDs are allocated *after* virtual extensions are. Once you upgrade to Wave ISM 1.5 SP2 or higher, existing SIP station IDs will change, because there are now 1024 'preallocated' virtual extensions, instead of 500. Station IDs are displayed when a user logs on to the User/Group Management applet or ViewPoint. *Be sure to make SIP phone users who specify station IDs when logging in, or who have shortcuts that reference station ID aware of this change.*

To configure virtual extensions

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the User/Group Management icon, located in the PBX Administration section. Log in to the User/Group Management applet when it opens in the remote session window.
3. Click **File > New User** to open the User dialog.
4. Enter appropriate name information.
5. Enter an **Extension** number.
6. Under **Associated device**, use the **Slot:port** section to select **No Slot Selected** and **No Port Selected** from the drop-down lists.
7. Select **Analog** from the **Telephone type** list.
8. On the User \ External Caller ID tab, select **Do Not Send Caller ID**.
9. Configure other user options as needed.
10. Click **OK** to close the Configure User dialog.

Configuring zone paging groups

Zone paging groups allow you to page a group of digital phones simultaneously. Zone paging groups are configured in the Zone Paging Groups applet. You can create up to 32 zone paging groups.

About SIP paging

SIP paging is integrated into Wave's zone paging feature. Multicast SIP paging is the preferred method, although both multicast and unicast SIP paging is supported.

	Multicast SIP paging	Unicast SIP paging
Supported on:	Edge Gigabit-E IP phones	Older Edge IP phones
Maximum phones paged simultaneously:	500	150
Resources required:	*No additional resources required.* The page goes out on a single stream to which the phones are subscribed.	*Requires one SIP phone resource per phone.*

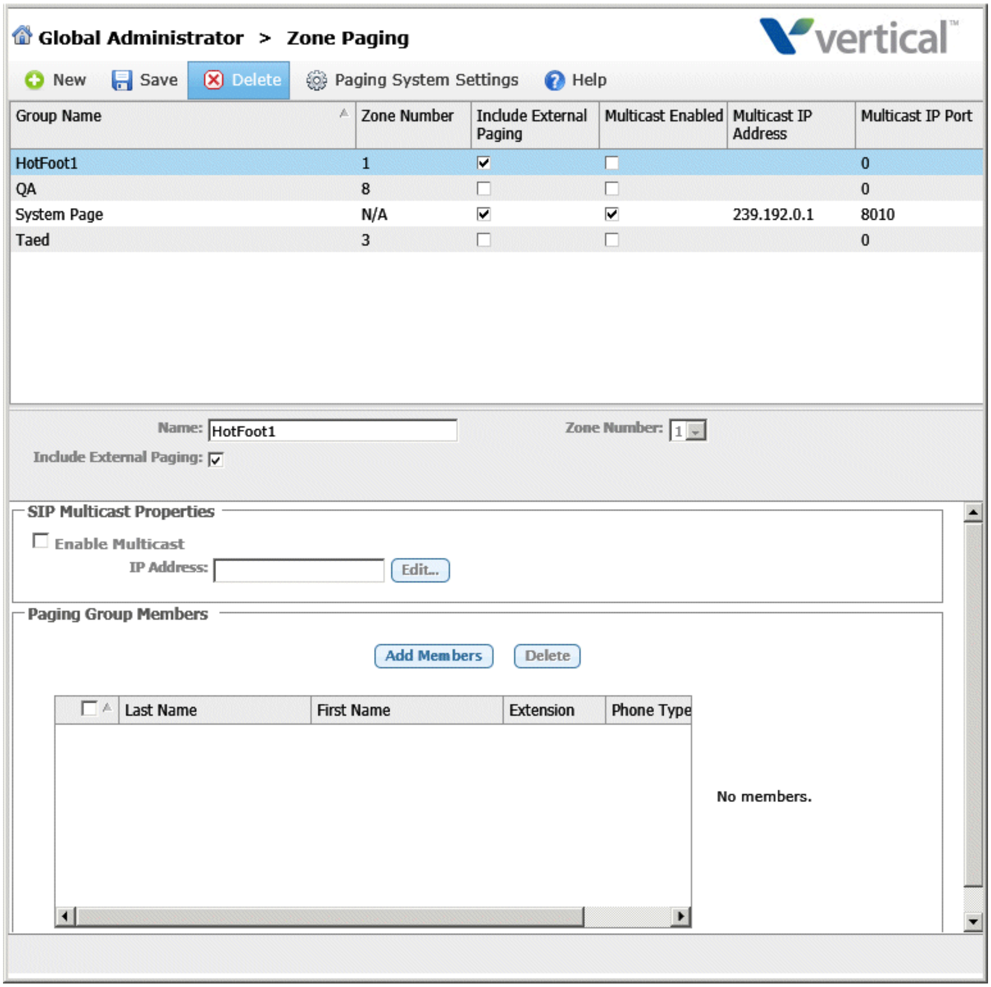
To create a zone paging group

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click Zone Paging Groups , located in the PBX Administration section.

3 Zone Paging Groups opens listing the zone paging groups created so far.



Global Administrator > Zone Paging

Group Name	Zone Number	Include External Paging	Multicast Enabled	Multicast IP Address	Multicast IP Port
HotFoot1	1	☑	□		0
QA	8	□	□		0
System Page	N/A	☑	☑	239.192.0.1	8010
Taed	3	□	□		0

Name: HotFoot1

Zone Number: 1

Include External Paging: ☑

SIP Multicast Properties

□ Enable Multicast

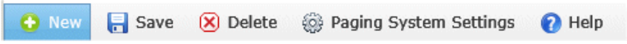
IP Address:

Paging Group Members

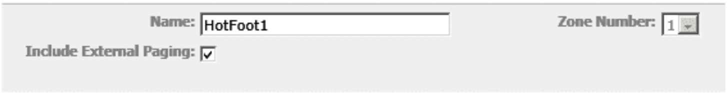
□	Last Name	First Name	Extension	Phone Type

No members.

4 Click **New** on the toolbar to create a new zone paging group.



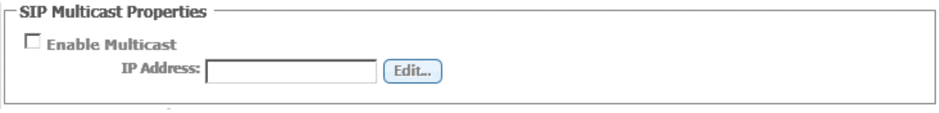
5 Enter the following information in the Details section:


Name: HotFoot1
Zone Number: 1
Include External Paging: ☑

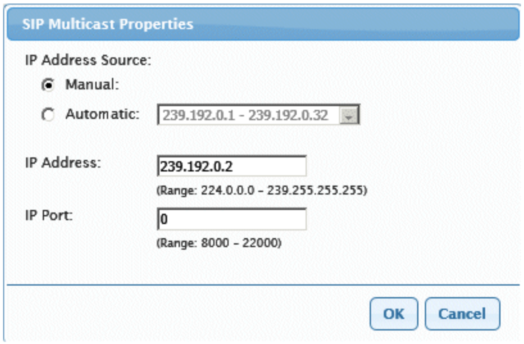
- **Name**. Select a zone number from the drop-down list, or accept the next unassigned zone number that is assigned automatically.
- **Zone Number.** Enter a descriptive name for the zone paging group.
- **Include External Paging**. Select this checkbox to also make an overhead page whenever a page is sent to this zone paging group.

  Note: To use this feature, you must have an external paging device on your system, and the Public Address feature must be enabled—see “Enabling Public Address” on page 16-26. Also, for a digital or SIP phone user to be able to send a page to a zone paging group, you must configure a System Page feature button on that digital phone—see “Page feature” on page 10-27.)

6 If this zone paging group will be used for SIP multicast SIP paging, select the **Enable Multicast** checkbox in the SIP Multicast Properties section:


SIP Multicast Properties
□ Enable Multicast
IP Address:

Accept the default **IP Address** (if shown), or click **Edit** to open the the SIP Multicast Properties dialog:



SIP Multicast Properties

IP Address Source:

● Manual:

○ Automatic: 239.192.0.1 - 239.192.0.32

IP Address: 239.192.0.2

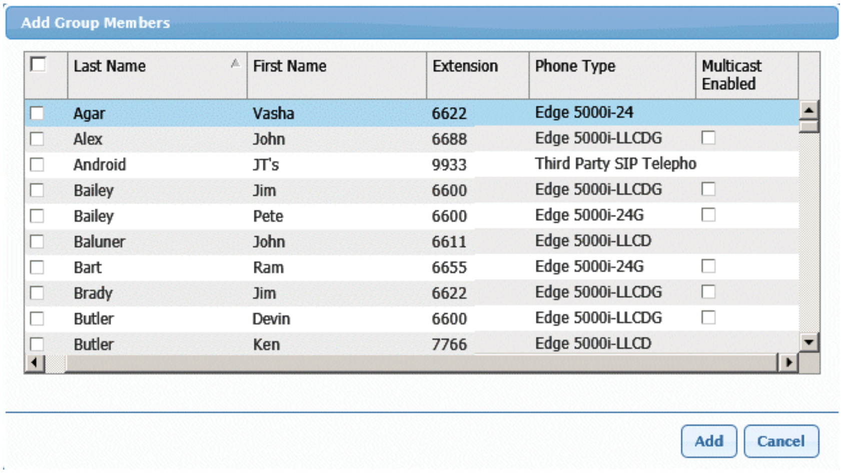
(Range: 224.0.0.0 - 239.255.255.255)

IP Port: 0

(Range: 8000 - 22000)

- **IP Address Source**. Do one of the following:
  - Click **Manual** to specify a single IP address to use. If you select **Manual**, enter that IP Address below.
  - Click **Automatic** to specify a range of IP addresses to use, then select a range from the drop-down list.
- **IP Address**. (Disabled if you select **Automatic**.)
- **IP Port.**

7 Click **Add** to add members to the zone paging group. The Add Zone Paging Group Members dialog opens listing the available extensions.



Add Group Members

☐	Last Name	First Name	Extension	Phone Type	Multicast Enabled
☐	Agar	Vasha	6622	Edge 5000i-24	
☐	Alex	John	6688	Edge 5000i-LLCDG	☐
☐	Android	JT's	9933	Third Party SIP Telepho	
☐	Bailey	Jim	6600	Edge 5000i-LLCDG	☐
☐	Bailey	Pete	6600	Edge 5000i-24G	☐
☐	Baluner	John	6611	Edge 5000i-LLCD	
☐	Bart	Ram	6655	Edge 5000i-24G	☐
☐	Brady	Jim	6622	Edge 5000i-LLCDG	☐
☐	Butler	Devin	6600	Edge 5000i-LLCDG	☐
☐	Butler	Ken	7766	Edge 5000i-LLCD	

Select one or more members from the list, and then click **OK** to add them to the group. For SIP phone users, select the **Multicast Enabled** checkbox.

Note: Only digital and SIP phones appear in the list—analog phones cannot be part of a zone paging group.

8 Click **Save** on the toolbar to save the new zone paging group.

Configuring instant messaging

Wave IMpulse allows users to send and receive instant messages via ViewPoint. Users can also exchange instant messages with users in Wave organizations other than their own, and invite other users to an instant messaging conference.

Wave IMpulse provides secure instant messaging because it requires a valid LAN (or VPN) account and ViewPoint login credentials, and does not support file transfers, avoiding problems with potential viruses.

Wave IMpulse limitations include the following:

- No coaching, monitoring, or recording of instant messages.
- No HIPPA compliance.
- No emoticon support.
- No custom statuses.

Configuring instant messaging in Wave consists of the following:

- Enabling the Instant Messaging server. See page 16-44.
- Setting up instant messaging permissions for users. See page 16-44.
- Using the Wave IMpulse Administrator Console to view the status of the Instant Messaging server; view the Error, Warning, Info, and Debug Logs; and perform other configuration options. See page 16-45.

Enabling the Instant Messaging server

After enabling the Instant Message server according to the following instructions, it may take up to 15 minutes for the server to be fully operational. For this reason, you should enable the server well in advance of when you want to use the Wave IMpulse Administrator Console, or when users will start sending instant messages.

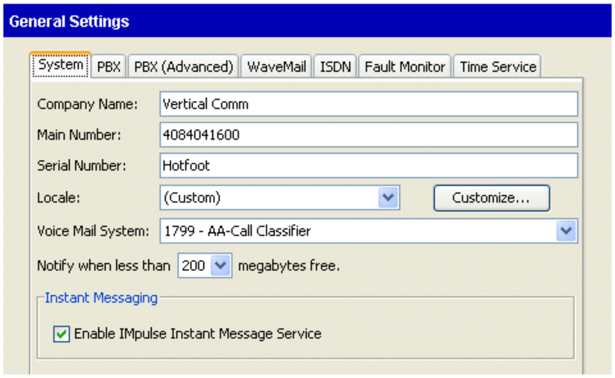
To enable the Instant Messaging server

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 On the System tab of the General Settings applet, select the **Enable Instant Messaging** check box.



General Settings

Company Name: Vertical Comm

Main Number: 4084041600

Serial Number: Hotfoot

Locale: (Custom)

Voice Mail System: 1799 - AA-Call Classifier

Notify when less than 200 megabytes free.

Instant Messaging

☑ Enable IMpulse Instant Message Service

Setting up instant messaging permissions for users

The following Wave permissions control a user’s ability to send and receive instant messages:

- **Allow Instant Messaging.** Controls the ability to send and receive instant messages in ViewPoint.

  Important! In order to avoid impacting system performance, you should only enable the **Allow Instant Messaging** permission for users who actually use IM.

One way to control this is to use a security role to turn off IM for the following:

- All virtual users. A virtual user is a user that does not have a Wave ISM User license assigned, and has a **Slot:port** setting of None on the User tab in User/Group Management. Virtual users are often used for routing purposes.
- Fax and credit card machines
- Break room and loading dock phones
- Any other user who does not use IM

See “Managing roles” on page 11-122. Also, turn off IM for

- **Allow inter-organizational Instant Messaging**. Controls the ability to send and receive instant messages with users in other Organizations configured in Wave. The **Allow Instant Messaging** permission must be enabled in order to send and receive inter-organizational instant messages.

You can apply these permissions to users in any of the following ways:

- **To an individual user**. See “The Security \ Permissions tab” on page 11-96.
- **To all users who are members of a role**. See “Creating a new role” on page 11-123.
- **To all users based on a user template**. See “User Templates dialog tabs” on page 11-109.

Using the Wave IMpulse Administrator Console

This section describes how to start the Wave IMpulse Administrator Console and how you can use it. See the following sections for details on how to perform specific tasks:

- “Specifying security settings” on page 16-49.
- “Generating and applying SSL server certificates” on page 16-51
- “Using content filters” on page 16-53
- “Configuring instant messaging archiving settings” on page 16-56
- “Searching the Instant Messaging archive” on page 16-57
- “Monitoring the status of Instant Messaging users” on page 16-58
- “Monitoring active client sessions” on page 16-59
- “Monitoring active server sessions” on page 16-60
- “Disabling and enabling Wave IMpulse over WaveNet” on page 16-60.

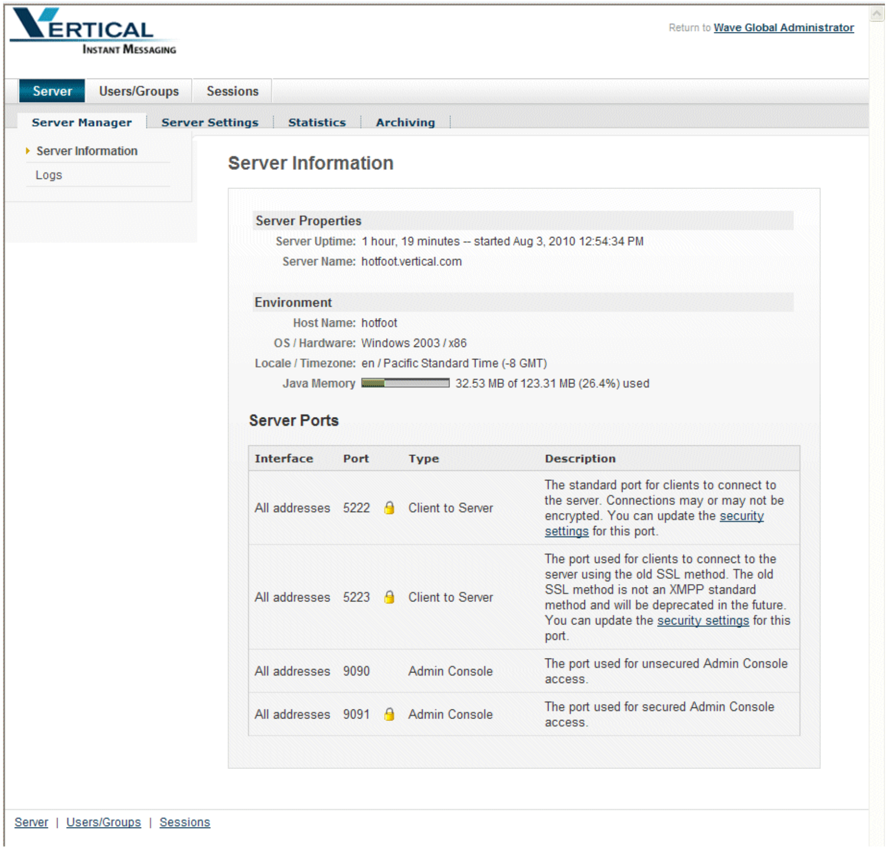
To start the Wave IMpulse Administrator Console

1 If necessary, click the Applications tab of the Management Console.

Click

2 Click the Wave IMpulse icon, located in the Unified Communications section.

The Wave IMpulse Administrator Console opens:



VERTICAL Instant Messaging

Return to Wave Global Administrator

Server Information

Server Properties

Server Uptime: 1 hour, 19 minutes -- started Aug 3, 2010 12:54:34 PM
Server Name: hotfoot.vertical.com

Environment

Host Name: hotfoot
OS / Hardware: Windows 2003 / x86
Locale / Timezone: en / Pacific Standard Time (-8 GMT)
Java Memory 32.53 MB of 123.31 MB (26.4%) used

Server Ports

Interface	Port		Type	Description
All addresses	5222	🔒	Client to Server	The standard port for clients to connect to the server. Connections may or may not be encrypted. You can update the security settings for this port.
All addresses	5223	🔒	Client to Server	The port used for clients to connect to the server using the old SSL method. The old SSL method is not an XMPP standard method and will be deprecated in the future. You can update the security settings for this port.
All addresses	9090		Admin Console	The port used for unsecured Admin Console access.
All addresses	9091	🔒	Admin Console	The port used for secured Admin Console access.

Server | Users/Groups | Sessions

3 Click on one of the main tabs (**Server**, **Users**, or **Sessions**) and then click on one of the sub-tabs to see the available pages.

Note: Not all of the available sub-tabs and pages are described in the following table. See the indicated sections for more information.

Main tab	Sub-tab	Page
Server	**Server Manager**	**Server Information**. This page opens when you start the Vertical Instant Messaging administrator console. It provides important information about the Instant Messaging server properties, environment, and port usage: • **Server Uptime**. Amount of time the Instant Messaging service has been running. • **Server Name**. Wave Server’s IP address. • **Host Name**. Host name of the Wave Server. • **OS/Hardware**. “Windows 2003 / x86” in this version. • **Locale/Timezone**. Wave Server’s time zone. • **Java Memory**. Snapshot of the amount of memory currently being used by the Java Virtual Machine running the Instant Messaging service. • **Server Ports**. Information about ports used by the Instant Messaging service. **Logs**. Use this page to view the Error, Warn, Info, and Debug Logs. (The Debug Log is disabled by default.)
	Server Settings	**Offline Messages**. Use this page to specify an offline message policy on how to handle instant messages when they are sent to a user who is not logged in. For example, you can store offline messages for later delivery, bounce offline messages back to the sender, and so forth. **Security Settings**. Clients can connect to the server using secured or unsecured connections. Use this page to specify how clients can connect to the server. See “Specifying security settings” on page 16-49. You also use these settings to disable and enable Wave IMpulse over WaveNet. See page 16-60. **Server Certificates**. Use this page to generate self-signed SSL server certificates or apply a signed SSL server certificate issued by a Certification Authority (CA). See “Generating and applying SSL server certificates” on page 16-51 for best-practice recommendations. **Content Filters**. Use this page to define criteria that determine how instant messages are handled based on message content. See “Using content filters” on page 16-53.

Main tab	Sub-tab	Page
	Statistics	**Statistics**. Use this page to view a snapshot of the current activity on the Instant Messaging server. **All Reports**. Use this page to view graphic reports on various aspects of instant messaging activity. You can also download the reports in PDF format.
	Archiving	**Search Archive**. Use this page to search the Instant Messaging archive by participant, date range, or keyword. See “Searching the Instant Messaging archive” on page 16-57. **Archiving Settings**. Use this page to manage archiving settings. You can archive information about instant messaging activity, message content, or both. You also use this page to: • Specify the number of minutes a conversation can be idle and the maximum number of minutes a conversation can last before the conversation is ended. • View index statistics. • Rebuild the current index used to search the archive. See “Configuring instant messaging archiving settings” on page 16-56. **Conversations**. You use this page to monitor active conversations.
User	**Users**	**User Summary**. Use this page to view a summary of all Wave users who have been given permission to send and receive instant messages (as described in “Setting up instant messaging permissions for users” on page 16-44.) You can also see which users are currently online, and when they last logged out (if they are offline). See “Monitoring the status of Instant Messaging users” on page 16-58.

Main tab	Sub-tab	Page
Sessions	**Active Sessions**	**Client Sessions**. Use this view-only page to monitor ViewPoint clients that are currently running and connected to the Instant Messaging server. See “Monitoring active client sessions” on page 16-59. **Server Sessions**. Use this view-only page to monitor current active connections between WaveNet nodes on which the Instant Messaging service is currently running. Note that nodes may not appear in this list until an instant message or presence information is sent between nodes. See “Monitoring active server sessions” on page 16-60.

4 Click **Wave Global Administrator** at the upper right of the screen to close the Instant Messaging administrator console.

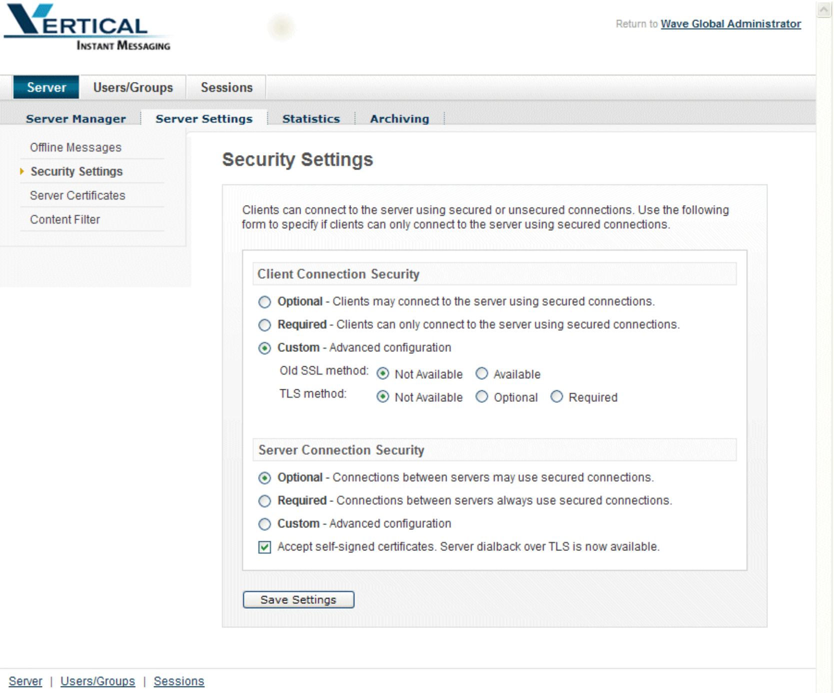
Specifying security settings

Clients can connect to the server using secured or unsecured connections. Use this page to specify how clients can connect to the server.

To specify security settings

1 Start the Wave IMpulse Administrator Console according to the instructions in “Using the Wave IMpulse Administrator Console” on page 16-45.

2 Select **Server > Server Settings > Security Settings**. The Security Settings page opens:



Security Settings

Clients can connect to the server using secured or unsecured connections. Use the following form to specify if clients can only connect to the server using secured connections.

Client Connection Security

○ **Optional** - Clients may connect to the server using secured connections.

○ **Required** - Clients can only connect to the server using secured connections.

● **Custom** - Advanced configuration

Old SSL method: ● Not Available ○ Available

TLS method: ● Not Available ○ Optional ○ Required

Server Connection Security

● **Optional** - Connections between servers may use secured connections.

○ **Required** - Connections between servers always use secured connections.

○ **Custom** - Advanced configuration

☑ Accept self-signed certificates. Server dialback over TLS is now available.

3 In the Client Connection Security section, select one of the following:

- **Optional**.
- **Required**.
- **Custom**. Select this option if you need to specify advanced client connection security options.

4 If you selected **Custom**, specify one of the following:

- **Old SSL method**.
  - **Not Available**.
  - **Available**.
- **TLS method**.
  - **Not Available**.
  - **Optional**.
  - **Required**.

5 In the Server Connection Security section, select one of the following:

- **Optional**. Select this option if connections between servers may use secured connections.
- **Required**. Select this option if connections between servers must always use secured connections.
- **Custom**. Select this option if you need to specify advanced server connection security options.

6 Click **Save Settings**.

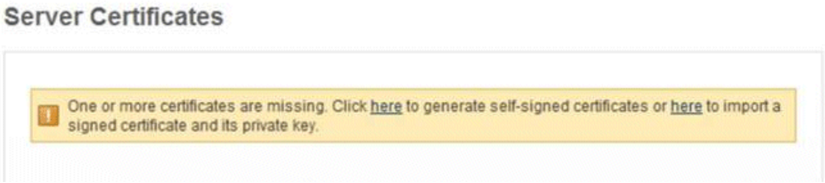
Generating and applying SSL server certificates

Secure Sockets Layer (SSL) negotiates point-to-point security between a client and a server, and is the dominant security protocol for Internet monetary transactions and communications. An SSL server certificate (a password-protected, encrypted data file), allows entities exchanging data to authenticate each other.

There are two kinds of SSL server certificates:

- **Signed SSL certificates** provide the highest level of security. You obtain a signed server certificate from an issuing Certificate Authority (CA), who guarantees that the identity of the individual or entity granted the certificate is as claimed. Once you receive your signed SSL server certificate, you import and apply it via the Wave IMpulse Administrator Console according to the instructions in this section.
- **Self-signed server certificates** are generated automatically by Wave.

If for any reason you need to generate a self-signed SSL server certificate or import a signed SSL server certificate, a message similar to the following is displayed at the top of the Server Certificates page. Click the link or links provided to perform the required action.



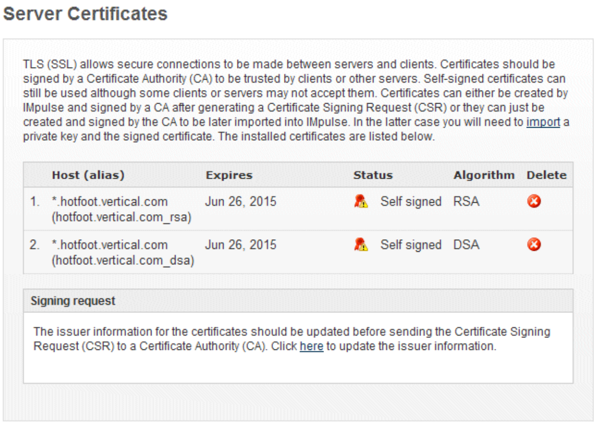
Server Certificates

One or more certificates are missing. Click here to generate self-signed certificates or here to import a signed certificate and its private key.

To generate or apply a server certificate

1 Start the Wave IMpulse Administrator Console according to the instructions in “Using the Wave IMpulse Administrator Console” on page 16-45.

2 Select **Server > Server Settings > Server Certificates**. The Server Certificates page opens:



Server Certificates

TLS (SSL) allows secure connections to be made between servers and clients. Certificates should be signed by a Certificate Authority (CA) to be trusted by clients or other servers. Self-signed certificates can still be used although some clients or servers may not accept them. Certificates can either be created by IMpulse and signed by a CA after generating a Certificate Signing Request (CSR) or they can just be created and signed by the CA to be later imported into IMpulse. In the latter case you will need to import a private key and the signed certificate. The installed certificates are listed below.

	Host (alias)	Expires	Status	Algorithm	Delete
1.	*.hotfoot.vertical.com (hotfoot.vertical.com_rsa)	Jun 26, 2015	Self signed	RSA	☒
2.	*.hotfoot.vertical.com (hotfoot.vertical.com_dsa)	Jun 26, 2015	Self signed	DSA	☒

Signing request

The issuer information for the certificates should be updated before sending the Certificate Signing Request (CSR) to a Certificate Authority (CA). Click here to update the issuer information.

Current SSL server certificates are listed.

3 Respond to any requests listed at the bottom of the page by clicking on the provided link.

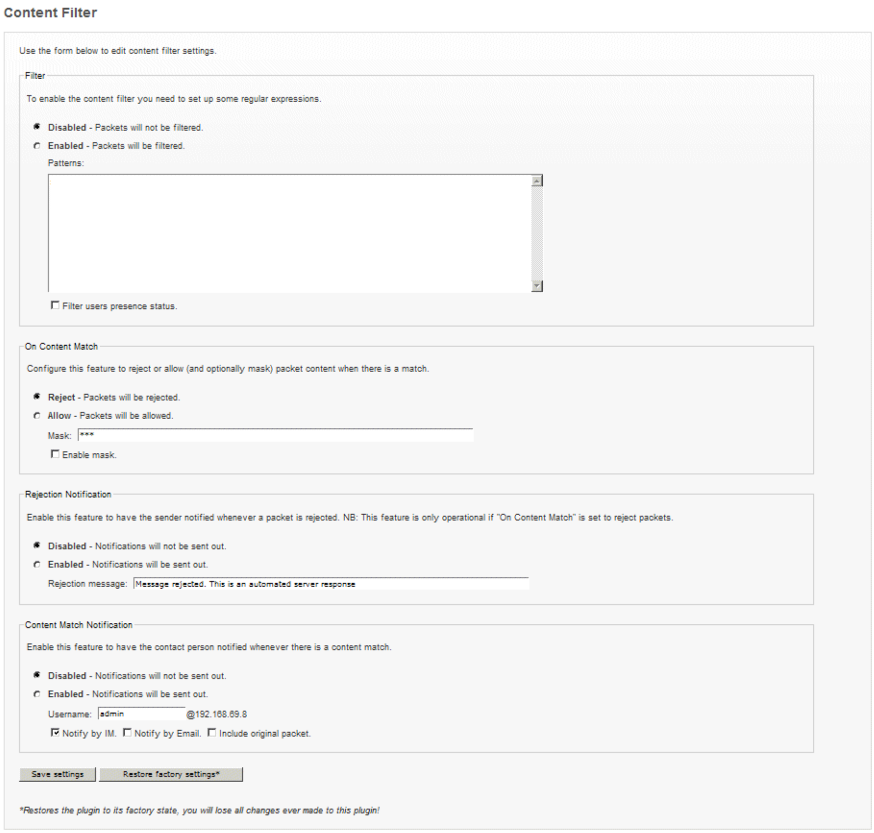
Using content filters

You use this page to create filters that modify how instant messages are handled based on their content. For example, you could create a filter to prevent Social Security Numbers, account numbers, or other sensitive information from being passed along via an instant message. If message content matches the filter, you can reject the message, allow it, or allow it and replace the matching content with a text string that you specify. Optionally, you can notify the sender if a message was rejected, or notify a contact person when a content match occurs.

To create a content filter

1 Start the Wave IMpulse Administrator Console according to the instructions in “Using the Wave IMpulse Administrator Console” on page 16-45.

2 Select **Server > Server Settings > Content Filter**. The Content Filter page opens:



Content Filter

Use the form below to edit content filter settings.

Filter

To enable the content filter you need to set up some regular expressions.

● **Disabled** - Packets will not be filtered.
○ **Enabled** - Packets will be filtered.

Patterns:

□ Filter users presence status.

On Content Match

Configure this feature to reject or allow (and optionally mask) packet content when there is a match.

● **Reject** - Packets will be rejected.
○ **Allow** - Packets will be allowed.

Mask: ***

□ Enable mask.

Rejection Notification

Enable this feature to have the sender notified whenever a packet is rejected. NB: This feature is only operational if "On Content Match" is set to reject packets.

● **Disabled** - Notifications will not be sent out.
○ **Enabled** - Notifications will be sent out.

Rejection message: Message rejected. This is an automated server response

Content Match Notification

Enable this feature to have the contact person notified whenever there is a content match.

● **Disabled** - Notifications will not be sent out.
○ **Enabled** - Notifications will be sent out.

Username: admin @192.168.69.8

☑ Notify by IM. □ Notify by Email. □ Include original packet.

Restores the plugin to its factory state, you will lose all changes ever made to this plugin!

3 In the **Filter** section, you enable or disable the content filter and enter the regular expressions that make up the filter.

- **Disabled**. Select this checkbox to inactivate the content filter so that it is not applied to instant message traffic.
- **Enabled**. Select this checkbox to activate the content filter so that it is applied to instant message traffic.
- **Patterns**. Enter the content that you want to filter on. You can enter one or more regular expressions. Separate multiple regular expressions with commas.

  There are many elements that can go into creating a content filter pattern, but here are some examples:

  - **Social Security number:** `\d{3}-\d{2}-\d{4}`
  - **10-digit phone number:** `[(]?\d{3}[\s-)]*?\d{3}[-]?\d{4}`
  - **Words** similar to “restrict”, including “restricting”, “restricted”, and so forth: `restrict[\w]*?`

4 In the **On Content Match** section, you specify the action that will occur when there is a content match.

- **Reject**. Select this checkbox to reject the message if there is a content match.
- **Allow**. Select this checkbox to allow the message if there is a content match.
  - **Mask.** Optionally, enter the text string that will replace the matching content in the message.
  - **Enable mask**. Select this checkbox to enable the mask.

5 In the **Rejection Notification** section, you specify whether or not to notify the sender when a message is rejected due to a content match.

- **Disabled**. Select this checkbox if you do not want to notify the sender that a message has been rejected due to a content match.
- **Enabled**. Select this checkbox to notify a user that a message has been rejected due to a content match.
  - **Rejection message**. Enter the text of the rejection message.

6. In the **Content Match Notification** section, you identify the contact person to whom a notification will be sent whenever there is a content match.
   - **Disabled**. Select this checkbox if you do not want to notify the contact when there is a content match.
   - **Enabled**. Select this checkbox to automatically notify the contact when there is a content match.
     - **Username**. Enter the name of the user to notify.
     - **Notify by IM**. Select this checkbox to notify the contact via an instant message.
     - **Notify by Email**. Select this checkbox to notify the contact via e-mail.
     - **Include original packet**. Select this checkbox to include the original message in the notification, before any mask was applied.
7. Click **Save Settings** to save the content filter.

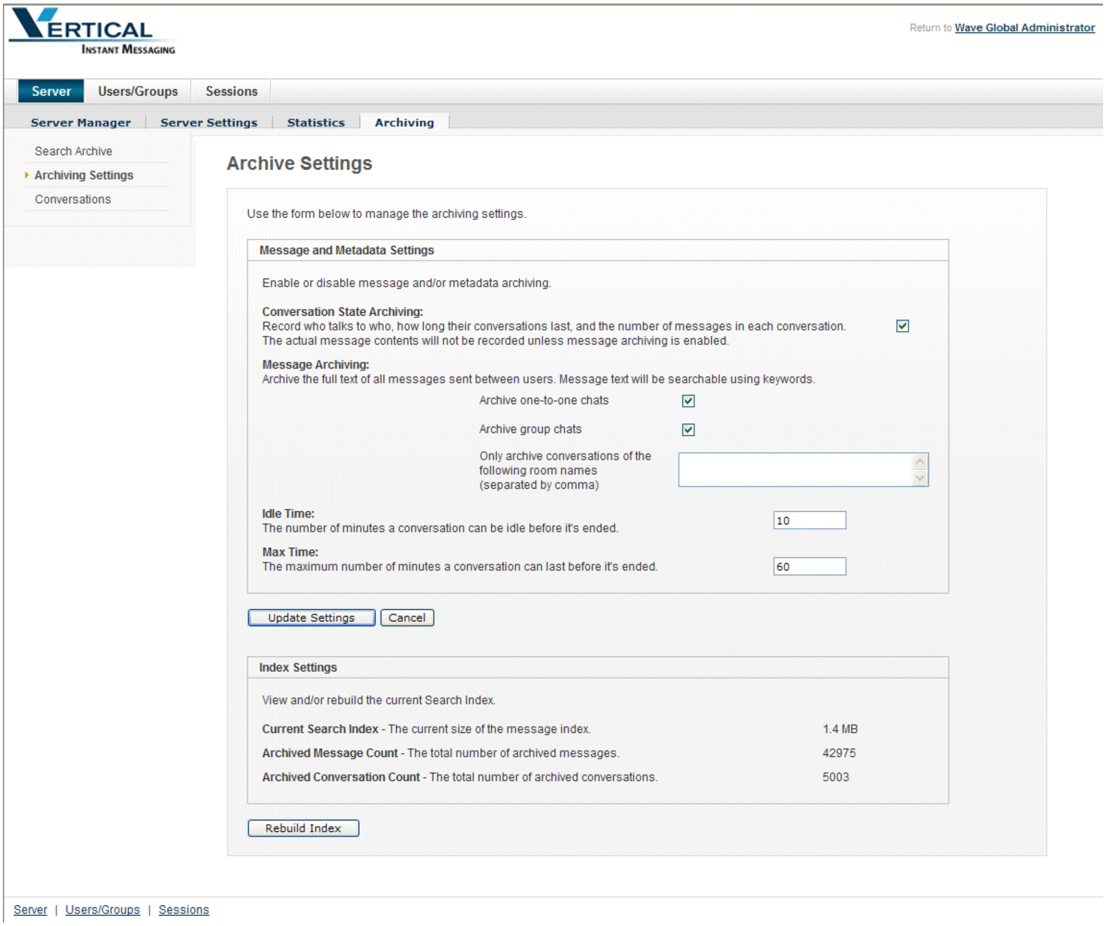
Configuring instant messaging archiving settings

For information on how to search the archive by participant, date range, or keyword, see "Searching the Instant Messaging archive" on page 16-57.

To configure Instant Messaging archiving settings

1 Start the Wave IMpulse Administrator Console according to the instructions in "Using the Wave IMpulse Administrator Console" on page 16-45.

2 Select **Server > Archiving > Archiving Settings**. The Archiving Settings page opens:



Archive Settings

Use the form below to manage the archiving settings.

Message and Metadata Settings

Enable or disable message and/or metadata archiving.

Conversation State Archiving:
Record who talks to who, how long their conversations last, and the number of messages in each conversation. The actual message contents will not be recorded unless message archiving is enabled. ☑

Message Archiving:
Archive the full text of all messages sent between users. Message text will be searchable using keywords.

Archive one-to-one chats ☑

Archive group chats ☑

Only archive conversations of the following room names (separated by comma)

Idle Time:
The number of minutes a conversation can be idle before it's ended. 10

Max Time:
The maximum number of minutes a conversation can last before it's ended. 60

Index Settings

View and/or rebuild the current Search Index.

Current Search Index - The current size of the message index.	1.4 MB
Archived Message Count - The total number of archived messages.	42975
Archived Conversation Count - The total number of archived conversations.	5003

3 In the Message and Metadata Settings section, use the following settings to identify how much and what type of information to archive:

- **Conversation State Archiving**. Select this checkbox to archive information about instant messaging activity, including who talks to who, how long conversations last, and the number of messages in each conversation.
- **Message Archiving**. Select this checkbox to archive the full text of all messages sent between users. You can customize this setting further using the following settings:
- **Idle Time**. Enter the number of minutes a conversation can be idle before it is ended automatically.
- **Max Time**. Enter the number of minutes a conversation can last before it is ended automatically.

4 Click **Update Settings** to save your changes to the Message and Metadata Settings section.

5 In the Index Settings section, you can view the following information about the current archive index:

- **Current Search Index**. Current size of the archive.
- **Archived Message Count**. Total number of currently archived messages.
- **Archived Conversation Count**. Total number of currently archived conversations.

Searching the Instant Messaging archive

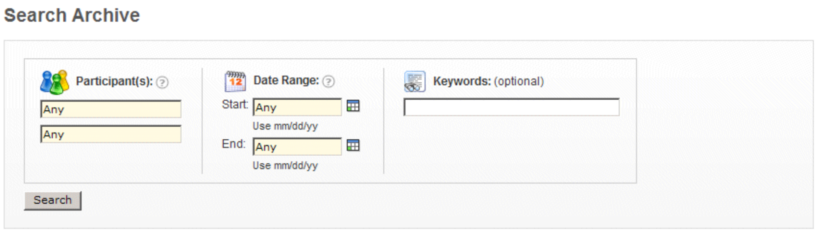
You can search the Instant Messaging archive by participant, date range, or keyword.

For information on how to configure archiving settings to control the amount and type of information archived, see “Configuring instant messaging archiving settings” on page 16-56.

To search the Instant Messaging archive

1 Start the Wave IMpulse Administrator Console according to the instructions in “Using the Wave IMpulse Administrator Console” on page 16-45.

2 Select **Server > Archiving > Search Archive**. The Search Archive page opens:



Search Archive

Participant(s): Any Any

Date Range: Start: Any Use mm/dd/yy End: Any Use mm/dd/yy

Keywords: (optional)

3 Select one or more of the following search criteria:

- **Participants**. Enter one of more users, separated by commas. (To view a list of users, select **User/Groups > Users > User Summary**.)
- **Date Range**. Specify and **Start** and **End** date range.
- **Keywords**. Enter one or more keywords to search for, separated by commas.

4 Click **Search** to search the archive using the criteria specified.

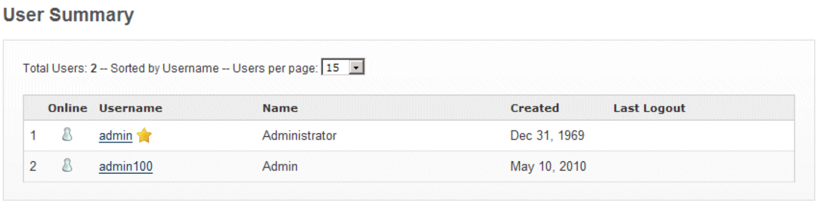
Monitoring the status of Instant Messaging users

You can view a summary of all Wave users who have been given permission to send and receive Instant Messages (as described in "Setting up instant messaging permissions for users" on page 16-44.) You can also see which users are currently online, and when they last logged out (if they are offline).

To monitor the status of Instant Messaging users

1 Start the Wave IMpulse Administrator Console according to the instructions in "Using the Wave IMpulse Administrator Console" on page 16-45.

2 To monitor the status of users, select **User > Users > User Summary**. The User Summary page opens:



User Summary

Total Users: 2 -- Sorted by Username -- Users per page: 15

	Online	Username	Name	Created	Last Logout
1		admin ★	Administrator	Dec 31, 1969	
2		admin100	Admin	May 10, 2010	

3 The following information is displayed for each user:

- **Online**. Indicates the user's status:
  - User is currently online.
  - User is currently offline.
- **Username**.
- **Name**.
- **Created**.
- **Last Logout**.

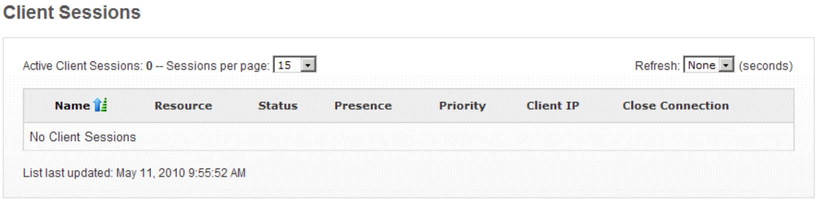
4 Click on a **Username** to view details for that user.

Monitoring active client sessions

To monitor active client sessions

1 Start the Wave IMpulse Administrator Console according to the instructions in “Using the Wave IMpulse Administrator Console” on page 16-45.

2 Select **Sessions > Active Sessions > Client Sessions**. The Client Sessions page opens:



Client Sessions

Active Client Sessions: **0** -- Sessions per page: 15

Refresh: None (seconds)

Name	Resource	Status	Presence	Priority	Client IP	Close Connection
No Client Sessions						

List last updated: May 11, 2010 9:55:52 AM

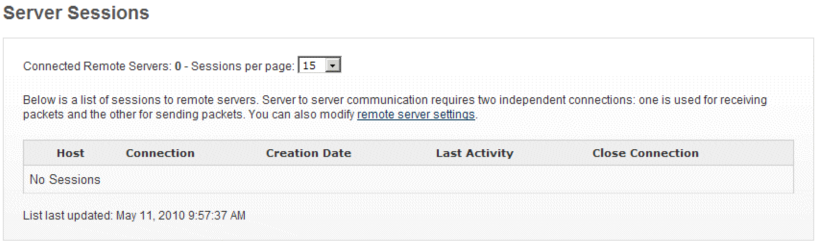
3 The following information is displayed for each active client session:

- **Name**.
- **Resource**.
- **Status**.
- **Presence**.
- **Priority**.
- **Client IP**.
- **Close Connection**.

Monitoring active server sessions

To monitor active server sessions

1. Start the Wave IMpulse Administrator Console according to the instructions in “Using the Wave IMpulse Administrator Console” on page 16-45.
2. Select **Sessions > Active Sessions > Server Sessions**. The Server Sessions page opens:



Server Sessions

Connected Remote Servers: **0** - Sessions per page: 15

Below is a list of sessions to remote servers. Server to server communication requires two independent connections: one is used for receiving packets and the other for sending packets. You can also modify remote server settings.

Host	Connection	Creation Date	Last Activity	Close Connection
No Sessions				

List last updated: May 11, 2010 9:57:37 AM

3. The following information is displayed for each active server session:
   - **Host.**
   - **Connection.**
   - **Creation Date.**
   - **Last Activity.**
   - **Close Connection.**

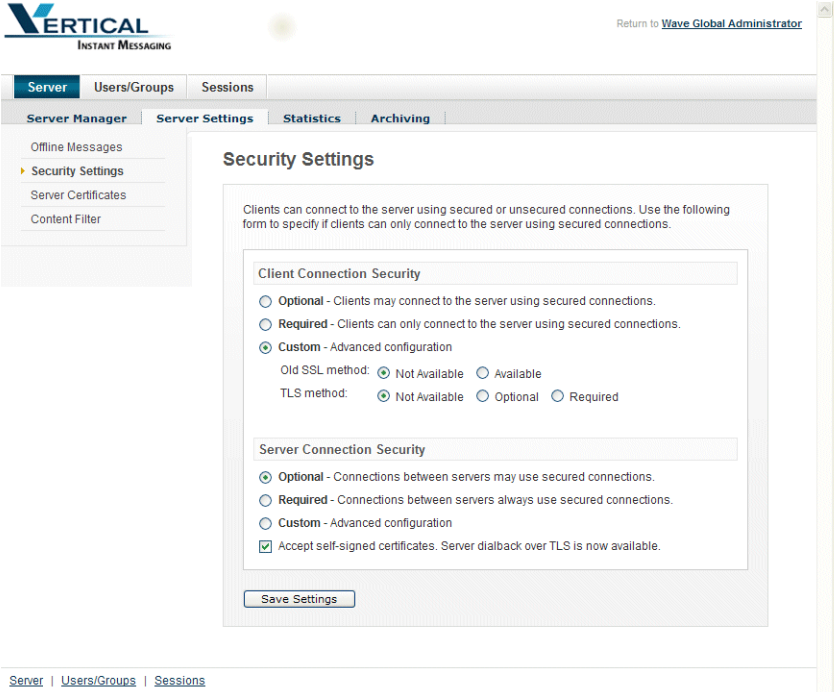
Disabling and enabling Wave IMpulse over WaveNet

Perform the following steps to disable Wave IMpulse communication between this and other WaveNet nodes. To re-enable Wave IMpulse over WaveNet, reverse the changes described in step 3 in the following procedure.

To disable Wave IMpulse over WaveNet

1 Start the Wave IMpulse Administrator Console according to the instructions in “Using the Wave IMpulse Administrator Console” on page 16-45.

2 Select **Server > Server Settings > Security Settings**. The Security Settings page opens:



Security Settings

Clients can connect to the server using secured or unsecured connections. Use the following form to specify if clients can only connect to the server using secured connections.

Client Connection Security

○ **Optional** - Clients may connect to the server using secured connections.

○ **Required** - Clients can only connect to the server using secured connections.

● **Custom** - Advanced configuration

Old SSL method: ● Not Available ○ Available

TLS method: ● Not Available ○ Optional ○ Required

Server Connection Security

● **Optional** - Connections between servers may use secured connections.

○ **Required** - Connections between servers always use secured connections.

○ **Custom** - Advanced configuration

☑ Accept self-signed certificates. Server dialback over TLS is now available.

3 In the Server Connection Security section, make the following changes:

a Select **Required**.

b Deselect the **Accept self-signed certificates. Server dialback over TLS is now available** checkbox.

4 Click **Save Settings**. Wave IMpulse communication between this and other WaveNet nodes will now fail, because by default WaveNet nodes use self-signed certificates.

Note: After re-enabling Wave IMpulse over WaveNet, users need to restart ViewPoint before they can start instant messaging across WaveNet nodes.

Chapter 17

Advanced Trunk and Channel Configuration

CHAPTER CONTENTS

This chapter provides information about configuring the advanced trunk and channel features.

Configuring advanced trunk settings

You can modify the advanced trunk settings for your T-1 trunk ports. You can find trunk Advanced Settings in the Trunk Configuration applet.

Caution! *These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

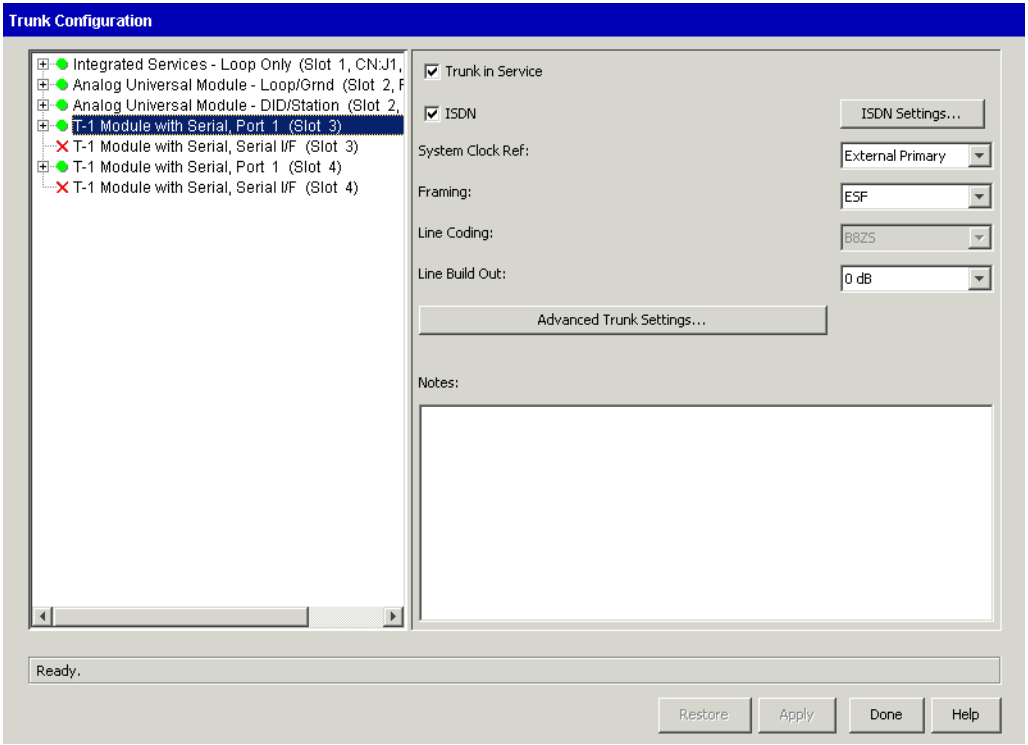
To configure advanced trunk settings for a T-1 module

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Select the T-1 module.



Trunk Configuration

- ⊞ ● Integrated Services - Loop Only (Slot 1, CN:J1,
- ⊞ ● Analog Universal Module - Loop/Grnd (Slot 2, F
- ⊞ ● Analog Universal Module - DID/Station (Slot 2,
- ⊞ ● T-1 Module with Serial, Port 1 (Slot 3)
- ✕ T-1 Module with Serial, Serial I/F (Slot 3)
- ⊞ ● T-1 Module with Serial, Port 1 (Slot 4)
- ✕ T-1 Module with Serial, Serial I/F (Slot 4)

☑ Trunk in Service

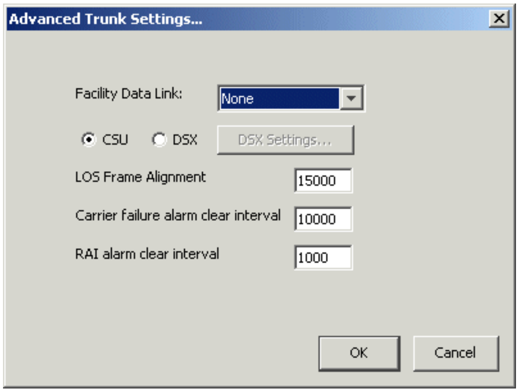
☑ ISDN

System Clock Ref:	External Primary
Framing:	ESF
Line Coding:	B8ZS
Line Build Out:	0 dB

Notes:

Ready.

4 Click **Advanced Trunk Settings.**



Advanced Trunk Settings...

Facility Data Link:	None

● CSU ○ DSX

LOS Frame Alignment	15000
Carrier failure alarm clear interval	10000
RAI alarm clear interval	1000

5 Set the **Facility Data Link** according to your Service Confirmation Letter.

Two Facility Data Link (FDL) protocols are available. You may select either protocol listed, both protocols, or no protocol.

- **T1.403.** Sends Performance Report Messages. The service provider can maintain a continuous history of trunk performance. The service provider can also send test messages to the trunk, if needed.
- **TR54016.** Sends messages when it is queried by the central office. If the service provider wants to know the status of a particular trunk, it will ask for it, and the Wave Server will send the information.
- **T1.403 & TR54016**
- **None**

This option is provided to allow the T-1 trunk to be tested and maintained by far-end equipment, for example, by the T-1 service provider's equipment.

Your trunk provisioning letter should include this information.

T-1 service providers try to guarantee the up time of the trunks they provide in two ways:

- They keep track of the physical layer errors in both directions, when possible, to proactively identify problems
- They send commands from their end of the T-1 to automatically loop T-1 trunks for error testing

You can view these messages in the trace log by using the Trace Monitor diagnostic applet in the Remote Diagnostics Console.

If you are configuring FDL on a public network, refer to the T-1 service provider's provisioning letter for information about the type of FDL support the service provider supports. If nothing is mentioned, select None.

If you are configuring FDL on a private network, you will typically select None. Since you control both of the T-1 endpoints, you can monitor statistics at each end.

If one trunk endpoint is not a Wave Server, select either T1.403 or TTR54016 according to what the management equipment supports on the non-Wave endpoint.

6 Choose one of the following settings:

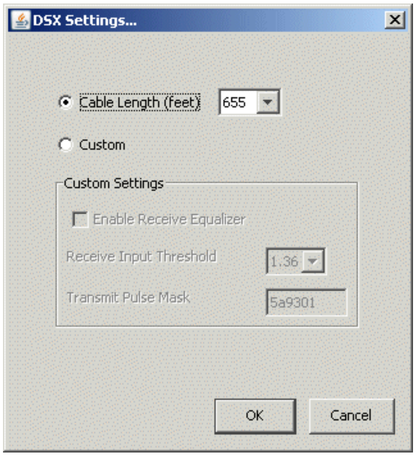
- **CSU**. Select this option if you are connecting to the PSTN. When connecting to the PSTN, the FCC **only** allows the use of CSU mode.

  Note: Although CSU mode was developed for the PSTN, it generally works well for private T-1 lines as well, as long as you do not need to set advanced signal strength and shape parameters.

  If you select CSU, go to step 10.

- **DSX**. Select this option **only** in a private network configuration where you are connecting one Wave Server to another Wave Server using this trunk. In DSX mode, you have full control of all the possible signal strength and shape parameters that can be configured for the T-1 trunk.

7 If you selected DSX mode, click **DSX Settings**.



DSX Settings...

● Cable Length (feet) 655

○ Custom

Custom Settings

□ Enable Receive Equalizer

Receive Input Threshold 1.36

Transmit Pulse Mask 5a9301

8 Enter the following information:

- **Cable Length (feet)**. Select the length of cable (in feet) to the other Wave Server.

  Note: Signal power level changes can be significant for short cable lengths, but not as much for longer lengths. Therefore, several short distance choices, and not as many long distant choices have been provided.

- **Custom**. Select this option to specify custom DSX settings. You should only change these settings if you are working with your service provider to determine the correct settings. Refer to “Customizing transmit and receive signal settings” on page 34-2 for more information on custom settings.

9 Click **OK** to return to the Advanced Trunk Settings dialog.

10 Modify the device timers settings, if appropriate, by typing new values in the text boxes. The value ranges and maximum number of digits allowed for these settings are:

- **LOS Frame Alignment.** Default=15000; Range=1000-30000
- **Carrier Failure Alarm Clear Interval.** Default=10000; Range=1000-15000
- **RAI Alarm Clear Interval.** Default=1000; Range=500-10000

11 Click **Apply** to save your changes.

12 Click **Done** to return to the Management Console.

Setting trunk timing values

Trunk timing values are classified as either inbound or outbound, depending on the direction of the call to which the timer applies.

Caution! *These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

- See “Setting digital trunk timing values” on page 17-6
- “Setting analog trunk timing values” on page 17-9

Setting digital trunk timing values

Caution! *These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

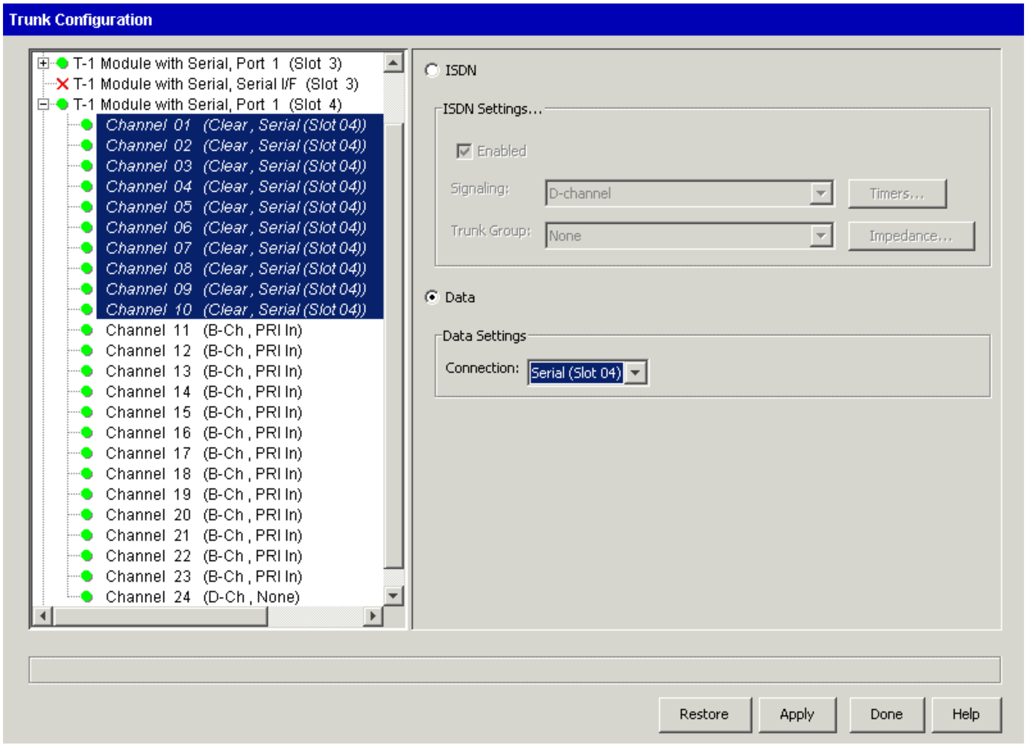
To set the timing values for a digital trunk

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Display and select the channel(s) you want to configure.



Trunk Configuration

- T-1 Module with Serial, Port 1 (Slot 3)
- T-1 Module with Serial, Serial I/F (Slot 3)
- T-1 Module with Serial, Port 1 (Slot 4)
  - Channel 01 (Clear, Serial (Slot 04))
  - Channel 02 (Clear, Serial (Slot 04))
  - Channel 03 (Clear, Serial (Slot 04))
  - Channel 04 (Clear, Serial (Slot 04))
  - Channel 05 (Clear, Serial (Slot 04))
  - Channel 06 (Clear, Serial (Slot 04))
  - Channel 07 (Clear, Serial (Slot 04))
  - Channel 08 (Clear, Serial (Slot 04))
  - Channel 09 (Clear, Serial (Slot 04))
  - Channel 10 (Clear, Serial (Slot 04))
  - Channel 11 (B-Ch, PRI In)
  - Channel 12 (B-Ch, PRI In)
  - Channel 13 (B-Ch, PRI In)
  - Channel 14 (B-Ch, PRI In)
  - Channel 15 (B-Ch, PRI In)
  - Channel 16 (B-Ch, PRI In)
  - Channel 17 (B-Ch, PRI In)
  - Channel 18 (B-Ch, PRI In)
  - Channel 19 (B-Ch, PRI In)
  - Channel 20 (B-Ch, PRI In)
  - Channel 21 (B-Ch, PRI In)
  - Channel 22 (B-Ch, PRI In)
  - Channel 23 (B-Ch, PRI In)
  - Channel 24 (D-Ch, None)

○ ISDN

ISDN Settings...

☑ Enabled

Signaling: D-channel

Trunk Group: None

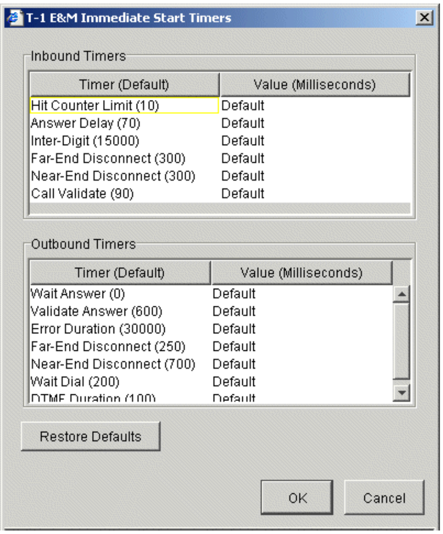
● Data

Data Settings

Connection: Serial (Slot 04)

4 Click **Timers**. Depending on the channel settings, one of the following dialogs opens:

- T-1 E&M Immediate Start Timers dialog



T-1 E&M Immediate Start Timers

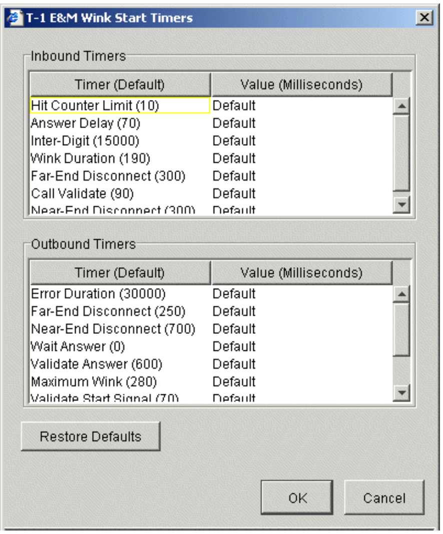
Inbound Timers

Timer (Default)	Value (Milliseconds)
Hit Counter Limit (10)	Default
Answer Delay (70)	Default
Inter-Digit (15000)	Default
Far-End Disconnect (300)	Default
Near-End Disconnect (300)	Default
Call Validate (90)	Default

Outbound Timers

Timer (Default)	Value (Milliseconds)
Wait Answer (0)	Default
Validate Answer (600)	Default
Error Duration (30000)	Default
Far-End Disconnect (250)	Default
Near-End Disconnect (700)	Default
Wait Dial (200)	Default
DTMF Duration (100)	Default

- T-1 E&M Wink Start Timers dialog



T-1 E&M Wink Start Timers

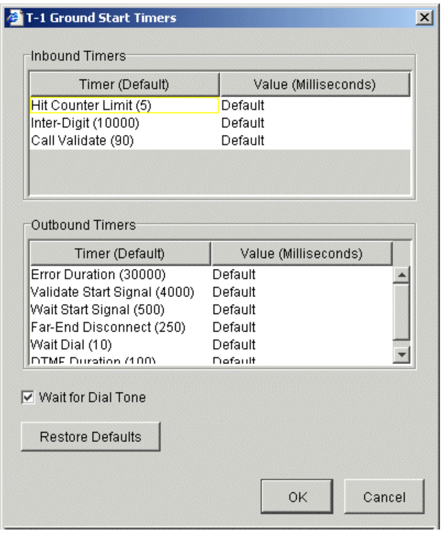
Inbound Timers

Timer (Default)	Value (Milliseconds)
Hit Counter Limit (10)	Default
Answer Delay (70)	Default
Inter-Digit (15000)	Default
Wink Duration (190)	Default
Far-End Disconnect (300)	Default
Call Validate (90)	Default
Near-End Disconnect (300)	Default

Outbound Timers

Timer (Default)	Value (Milliseconds)
Error Duration (30000)	Default
Far-End Disconnect (250)	Default
Near-End Disconnect (700)	Default
Wait Answer (0)	Default
Validate Answer (600)	Default
Maximum Wink (280)	Default
Validate Start Signal (70)	Default

- T-1 Ground Start Timers dialog



T-1 Ground Start Timers

Inbound Timers

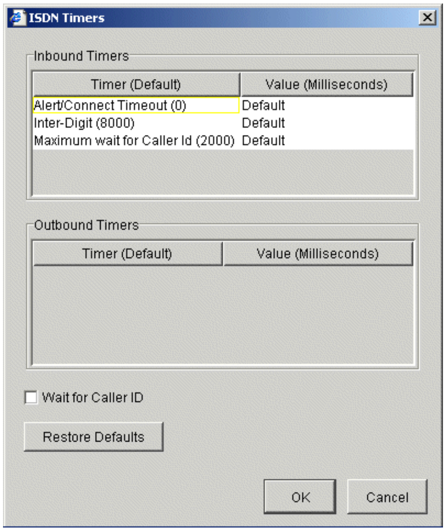
Timer (Default)	Value (Milliseconds)
Hit Counter Limit (5)	Default
Inter-Digit (10000)	Default
Call Validate (90)	Default

Outbound Timers

Timer (Default)	Value (Milliseconds)
Error Duration (30000)	Default
Validate Start Signal (4000)	Default
Wait Start Signal (500)	Default
Far-End Disconnect (250)	Default
Wait Dial (10)	Default
DTMF Duration (100)	Default

☑ Wait for Dial Tone

- ISDN Timers dialog



ISDN Timers

Inbound Timers

Timer (Default)	Value (Milliseconds)
Alert/Connect Timeout (0)	Default
Inter-Digit (8000)	Default
Maximum wait for Caller Id (2000)	Default

Outbound Timers

Timer (Default)	Value (Milliseconds)

☐ Wait for Caller ID

For information about specific T-1 trunk timers, refer to the tables in section “T-1 trunk timing values” on page 34-5.

5 Click the **Value** field of the timer that you want to edit. A text box opens where you can type a new value.

6 If the channel or channels you are editing are configured for Ground Start signaling, you can modify the **Wait For Dial Tone** setting by selecting or deselecting that check box.

This check box tells Wave whether or not to expect dial tone on the channel before dialing.

7 Click **Apply** to save your changes.

8 Click **Done** to return to the Management Console.

Setting analog trunk timing values

Caution! *These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

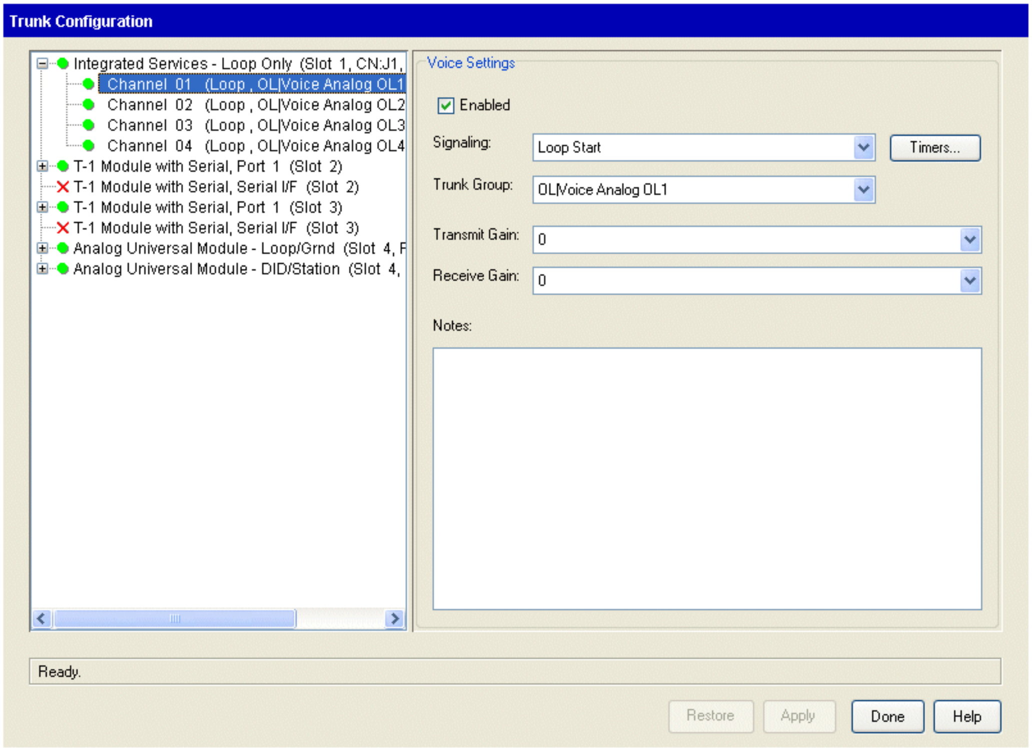
To set the timing values an analog trunks

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Display and select the channel(s) you want to configure.



Trunk Configuration

- ● Integrated Services - Loop Only (Slot 1, CN:J1,
  - ● Channel 01 (Loop , OL|Voice Analog OL1
  - ● Channel 02 (Loop , OL|Voice Analog OL2
  - ● Channel 03 (Loop , OL|Voice Analog OL3
  - ● Channel 04 (Loop , OL|Voice Analog OL4
- ● T-1 Module with Serial, Port 1 (Slot 2)
- ✕ T-1 Module with Serial, Serial I/F (Slot 2)
- ● T-1 Module with Serial, Port 1 (Slot 3)
- ✕ T-1 Module with Serial, Serial I/F (Slot 3)
- ● Analog Universal Module - Loop/Grnd (Slot 4, F
- ● Analog Universal Module - DID/Station (Slot 4,

Voice Settings

☑ Enabled

Signaling: Loop Start

Trunk Group: OL|Voice Analog OL1

Transmit Gain: 0

Receive Gain: 0

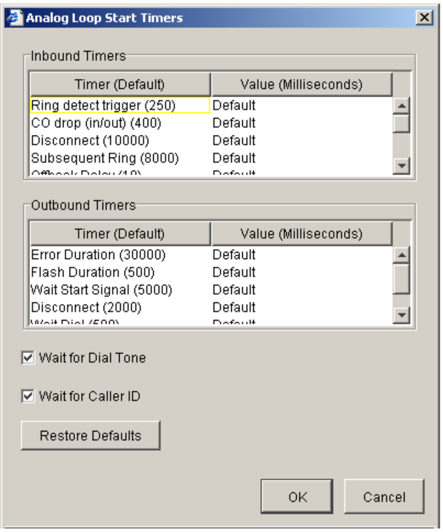
Notes:

Ready.

Note: You must select channels with the same Signaling configuration.

Depending on your signaling configuration for the selected trunks, you will see one of the following:

- Analog Loop Start Timers dialog



Analog Loop Start Timers

Inbound Timers

Timer (Default)	Value (Milliseconds)
Ring detect trigger (250)	Default
CO drop (in/out) (400)	Default
Disconnect (10000)	Default
Subsequent Ring (8000)	Default
Offhook Delay (10)	Default

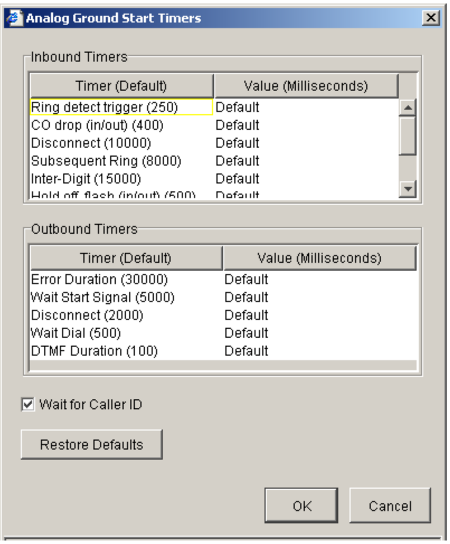
Outbound Timers

Timer (Default)	Value (Milliseconds)
Error Duration (30000)	Default
Flash Duration (500)	Default
Wait Start Signal (5000)	Default
Disconnect (2000)	Default
Wait Dial (500)	Default

☑ Wait for Dial Tone

☑ Wait for Caller ID

- Analog Ground Start Timers dialog



Analog Ground Start Timers

Inbound Timers

Timer (Default)	Value (Milliseconds)
Ring detect trigger (250)	Default
CO drop (in/out) (400)	Default
Disconnect (10000)	Default
Subsequent Ring (8000)	Default
Inter-Digit (15000)	Default
Hold off flash (in/out) (500)	Default

Outbound Timers

Timer (Default)	Value (Milliseconds)
Error Duration (30000)	Default
Wait Start Signal (5000)	Default
Disconnect (2000)	Default
Wait Dial (500)	Default
DTMF Duration (100)	Default

☑ Wait for Caller ID

4 Click the **Value** field of the timer that you want to edit. A text box opens where you can type a new value.

5 Enter a new value for the timer.

For information about specific analog trunk timers, refer to the tables in “Analog trunk timing values” on page 34-9.

6 If you are using Loop Start signaling, you can specify the **Wait for Dial Tone** setting by selecting or deselecting that check box.

This check box indicates whether Wave should expect a dial tone on the channel before dialing.

7 If you are using Loop Start signaling, select the **Wait for Caller ID** check box if you want to specify that the trunk should wait one ring for Caller ID information on an inbound call and answer on the second ring. (Caller ID information will come between the first and second rings.)

8 Click **Apply** to save your changes.

9 Click **Done** to return to the Management Console.

Configuring system-wide ISDN settings

System-wide ISDN settings enable you to specify company-wide information about your ISDN channels, including how long-distance and international calls are dialed when using ISDN.

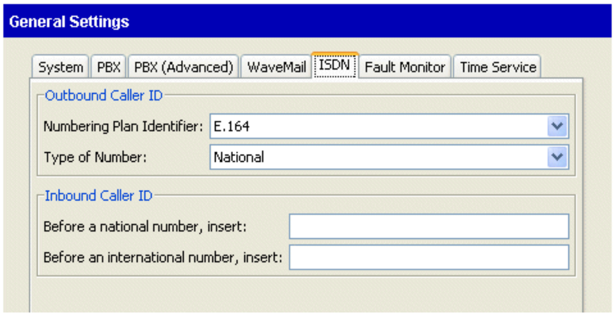
To set system-wide ISDN settings

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Click the ISDN tab.



Numbering Plan Identifier: E.164

Type of Number: National

Before a national number, insert:

Before an international number, insert:

4 In the Outbound Caller ID section, specify the **Numbering Plan Identifier** as specified in your Service Confirmation Letter from the drop-down list.

The numbering plan identifier (NPI) is used to indicate the general way phone numbers are constructed within the Caller ID. The two most common numbering plans are **E.164**—the world-wide ISDN numbering standard—and **Unknown**, indicating that the sender does not want to specify a plan. **Private** indicates that the calling party may use a unique string of digits for the calling party ID.

5 Specify the **Type of Number** as specified in your Service Confirmation Letter from the drop-down list.

Note that the numbering plan you selected in step 2 may have four types of numbers: Unknown, Subscriber (local), National (long distance), and International.

Caution! *This is an expert setting that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

6 In the Inbound Caller ID section, specify any digits to insert prior to a national number.

For example, when Wave receives a call specified as National, it prepends a 1 in the Caller ID that is sent, so the receiver will know how to correctly return the call, if necessary.

7 Specify any digits to insert prior to an international number.

For example, when Wave receives a call specified as International, it prepends a 011 in the Caller ID that is sent, so the receiver will know how to correctly return the call, if necessary.

8 Click **Apply** to save your changes.

9 Click **Done** to return to the Management Console.

Managing System Prompts and Audio

CHAPTER CONTENTS

System prompts are audio prompts that Wave plays to callers and users. System prompts offer callers menu choices and provide menus and instructions to users. You can use the standard prompts included with Wave Server, or record over them to create customized prompts.

This chapter explains how to play and rerecord the system prompts used throughout Wave Server.

To set up hold music, which enables callers to hear music whenever they are put on hold by a user or the system, see "Configuring Music On Hold" on page 16-21.

Presenting a confirmation prompt before voicemail

You can choose whether or not callers hear the prompt, "To leave a message press 1, or press * to return to the menu" after they hear a user's voicemail greeting. See "Setting general Wave settings" on page 4-4.

The System Prompts view

The System Prompts view in the User/Group Management applet allows you to listen to and change the recordings used for standard system prompts and auto attendants. For example, when you are setting up your Wave system, you typically go to this view to change the default Greeting prompt so that it contains your company name.

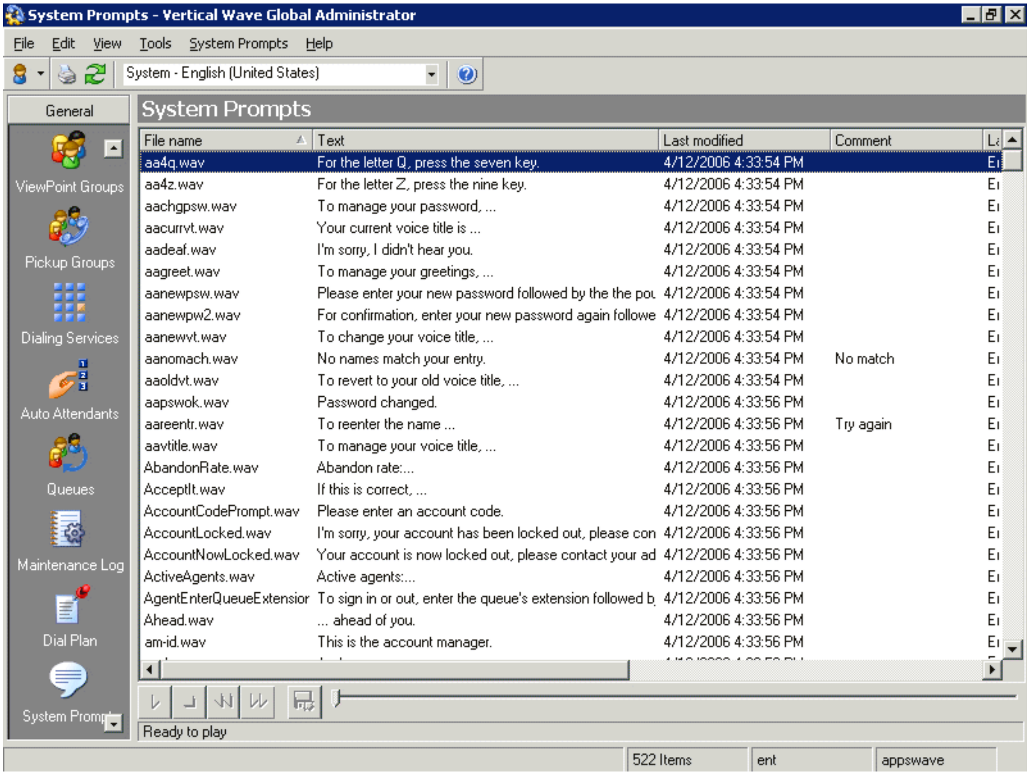
To display the System Prompts view

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Click the System Prompts button in the view bar to open the System Prompts view.



System - English (United States)

System Prompts

File name	Text	Last modified	Comment	La
aa4q.wav	For the letter Q, press the seven key.	4/12/2006 4:33:54 PM		Ei
aa4z.wav	For the letter Z, press the nine key.	4/12/2006 4:33:54 PM		Ei
aachgpsw.wav	To manage your password, ...	4/12/2006 4:33:54 PM		Ei
aacurrvt.wav	Your current voice title is ...	4/12/2006 4:33:54 PM		Ei
aadeaf.wav	I'm sorry, I didn't hear you.	4/12/2006 4:33:54 PM		Ei
aagreet.wav	To manage your greetings, ...	4/12/2006 4:33:54 PM		Ei
aanewpsw.wav	Please enter your new password followed by the the pou	4/12/2006 4:33:54 PM		Ei
aanewpw2.wav	For confirmation, enter your new password again followe	4/12/2006 4:33:54 PM		Ei
aanewvt.wav	To change your voice title, ...	4/12/2006 4:33:54 PM		Ei
aanomach.wav	No names match your entry.	4/12/2006 4:33:54 PM	No match	Ei
aaoldvt.wav	To revert to your old voice title, ...	4/12/2006 4:33:54 PM		Ei
aapswok.wav	Password changed.	4/12/2006 4:33:56 PM		Ei
aareentr.wav	To reenter the name ...	4/12/2006 4:33:56 PM	Try again	Ei
aavtitle.wav	To manage your voice title, ...	4/12/2006 4:33:56 PM		Ei
AbandonRate.wav	Abandon rate:...	4/12/2006 4:33:56 PM		Ei
AcceptIt.wav	If this is correct, ...	4/12/2006 4:33:56 PM		Ei
AccountCodePrompt.wav	Please enter an account code.	4/12/2006 4:33:56 PM		Ei
AccountLocked.wav	I'm sorry, your account has been locked out, please con	4/12/2006 4:33:56 PM		Ei
AccountNowLocked.wav	Your account is now locked out, please contact your ad	4/12/2006 4:33:56 PM		Ei
ActiveAgents.wav	Active agents:...	4/12/2006 4:33:56 PM		Ei
AgentEnterQueueExtensior	To sign in or out, enter the queue's extension followed b	4/12/2006 4:33:56 PM		Ei
Ahead.wav	... ahead of you.	4/12/2006 4:33:56 PM		Ei
am-id.wav	This is the account manager.	4/12/2006 4:33:56 PM		Ei

Ready to play

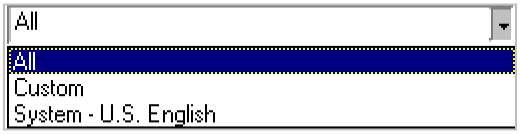
522 Items | ent | appswave

Each system prompt is displayed as a row in the view. The information in the following table is displayed for each system prompt.

Column	Description
File name	File name of the prompt.
Text	Contents of the file in text form. The text displayed here is accurate only if it is updated each time the file is changed. If you are unsure of the accuracy of the text, play the file to confirm what it says.
Last modified	Last time that the file was modified.
Comment	How the prompt is used in Wave. Applies to custom prompts and auto attendant prompts only. The column is blank for all other prompts.
Language	The set of language prompts to which this system prompt belongs. User-recorded prompts such as auto attendant prompts have this column blank.

Controlling the prompt display

By default the System Prompts view displays all system prompts on the Wave Server. Use the control on the toolbar if you want to display only the custom prompts you have recorded or only the prompts for a single language.



Managing system prompts

This section explains the following aspects of managing system prompts:

- Playing system prompts (see below)
- Exporting system prompt text (see page 18-4)
- Exporting and importing system prompt audio files (see page 18-5)

Playing system prompts

You can play system prompts over the phone to confirm that they contain the correct information. When you play a system prompt, your phone rings and the prompt plays when you answer. See “Using the audio controls” on page 2-21 for more information.

To play a system prompt

1 In the System Prompts view, select the name of the prompt that you want to play.

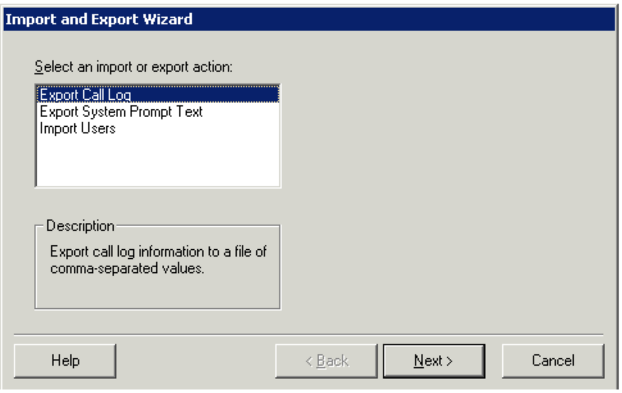
2 Choose **System Prompts > Play**.

Exporting system prompt text

Use the following procedure to export system prompt text into a CSV file for processing by a professional recording studio or for maintenance purposes.

To export system prompt text

1 In the System Prompts view, choose **File > Import and Export**. The Import and Export Wizard opens.



Import and Export Wizard

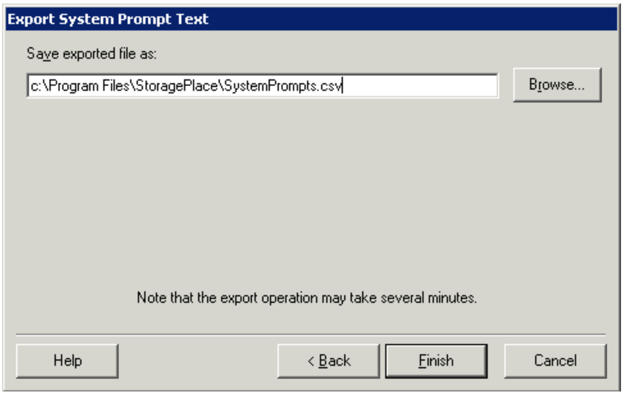
Select an import or export action:

Export Call Log
Export System Prompt Text
Import Users

Description

Export call log information to a file of comma-separated values.

2 Select **Export System Prompt Text** and click **Next**.



Export System Prompt Text

Save exported file as: c:\Program Files\StoragePlace\SystemPrompts.csv

Note that the export operation may take several minutes.

3 Under **Save exported file as**, accept the suggested location and file name or click **Browse** and choose a different location and enter a file name.

4 Click **Finish**. The file is exported.

Exporting and importing system prompt audio files

You can export a system prompt from your Wave Server for use on another. You also can import an existing sound file and use it as a system prompt. For more information, see “Importing and exporting voice files” on page 2-22.

Recording over system prompts

You may want to record over system prompts for any of the following reasons:

- You want your custom prompts and system prompts to be recorded with the same voice.
- You want to customize the message text of a prompt, for example, the Welcome message.
- You have access to voice talent that you prefer over the existing Wave voices.

Recording options

You can record system prompts in either of the following ways:

- Recording system prompts professionally (see page 18-7)
- Recording over system prompts yourself (see page 18-9)

About the recording process

To record a complete set of system prompts, you must do the following:

- Record the WAP file (see below).
- Build the indexed WAP file.
- Test the new prompts.
- Deploy the new prompts.

About the WAP and WAV files

Wave prompts are contained in the WAP file, an indexed file containing individual WAV recordings of variable information. Variable information, for example, numbers and dates, is used to build more complex prompts.

The WAP files are used together to produce the complete prompts that callers and users hear. For example, in the sentence prompt, “You have three new messages, and twelve saved messages”, the words “three” and “twelve” come from the WAP file.

The American English WAP files are located in the following directory:

```
C:\Program Files\Artisoft\TeleVantage Server\Vfiles\EN00
```

The American English WAP file is called `TVLEN00.WAP`.

About the sentence file

The sentence file is a text file that contains all the voice prompts and the sentences they form. The American English sentence file is located in the following location:

```
C:\Program Files\Artisoft\TeleVantage Server\TVLEN00.INI
```

Note: “EN00” identifies American English files.

Recording system prompts professionally

If you choose to obtain professional recordings, you should first choose a voice vendor with experience in telephony recording. Then:

- Select a voice.
- Provide the appropriate Wave files to the vendor in formats they can use.
- Test the new prompts for voice quality, usability, file-naming accuracy, and indexing accuracy.
- Deploy the new prompts.

Selecting a voice

The vendor will often provide you with 44kHz, full-bandwidth voice samples from which to choose. Ask your vendor to provide voice samples that have been re-sampled or recorded as MuLaw PCM Mono 8 kHz, which is the format used in Wave. This will ensure that your selection is based on how the voice will actually sound when used in your Wave system.

Keep in mind that high-pitched voices and high-frequency sounds degrade more as a result of this type of re-sampling, which may result in considerable change in higher frequency sounds at telephony bandwidth.

Using the standard Wave voices

To add or modify prompts using one of the standard Wave voices, contact Marketing Messages as shown in the following table. They provided the original set of prompts. Marketing Messages can record new voice files using the standard voices.

Language	Voice
U.S. English	“Ellen”
Latin American Spanish	“Claudia”
U. K. English	“Helen”
French Parisian	“Sylvie”
French Canadian	“Gisele”
German	“Anneli”

Contact Marketing Messages as follows:

Marketing Messages
51 Winchester Street
Newton, MA, U.S.A. 02461

800-486-4237 (phone)
617-527-3728 (fax)

http://www.marketingmessages.com

Providing files to the vendor

After you have selected a voice, you must provide your vendor with the list of prompt files and the text of each prompt to be recorded. The list of prompt files is available in the System Prompts and Prompts section of the TVLEN00.INI file.

You also need to provide your vendor with the TVLEN00.WAP file, so that your voice vendor can match the indexing of the new WAP file to the existing file.

Testing the new prompts

It is important that you thoroughly test all voice files that you receive from the vendor to ensure:

- Accuracy of file names
- Synchronization of written and spoken prompt content
- Quality of voice recording
- Accuracy of index order and format of the WAP file

See “Testing system prompts” on page 18-11 for information about using the Sentence Tester to assist with some of these tasks.

Deploying the new prompts

After all files are tested, you can replace the existing prompt files with the new ones. Place all new WAV files and the WAP file in the following directory:

```
C:\Program Files\Artisoft\TeleVantage Server\Vfiles\User
```

The following auto attendant prompts must also be copied to the User directory.

- `AACLOSED.WAV`
- `AAHI.WAV`
- `AA4SBN.WAV`
- `AAOPORWT.WAV`

The default location is `C:\Program Files\Artisoft\TeleVantage Server\Voice Files\EN00`.

Recording over system prompts yourself

When you record over system prompts yourself, you can record all of the WAV files as well as the WAP file, as with professional recording, or record just the WAV files and use the WAP file included with Wave.

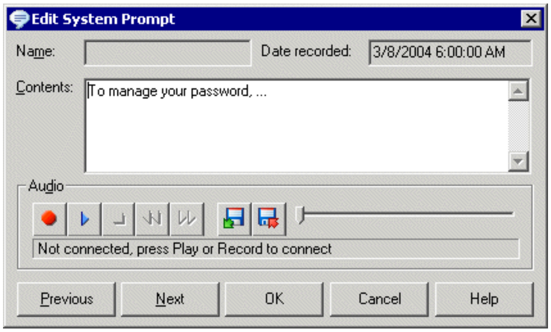
If you do not record over all the files, be aware that since prompts are combined with other prompts when presented to callers or users, recording some but not all prompts may result in a mismatch of voices between prompts or within the same prompt.

Recording over WAV files

To record over a prompt

1 In the System Prompts view, double-click the prompt. The Edit System Prompt dialog opens.

2 Under **Contents**, enter the text of the new prompt. Use this text as a script when you record the prompt.



Edit System Prompt

Name:

Date recorded: 3/8/2004 6:00:00 AM

Contents: To manage your password, ...

Not connected, press Play or Record to connect

3 Record the prompt. See “Using the audio controls” on page 2-21 for instructions.

4 Click **OK** to save the new version of the prompt.

Recording over the WAP file

You can record over the WAP file by using a variety of recording tools and WAP tools that can be found on the Internet.

Testing and deploying the new prompts

Use the Sentence Tester to test the new prompts. See “Testing system prompts” on page 18-11. For information about deploying the new prompts, see “Deploying the new prompts” on page 18-9.

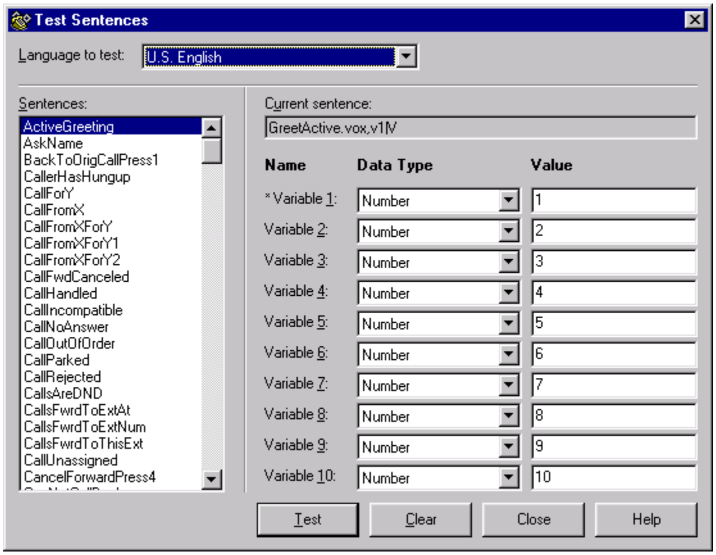
Testing system prompts

You can test system prompts by listening to them in context over your phone. By joining individual prompts into sentences and playing them as they are used in Wave, you can evaluate intonation, emphasis, and consistency.

To test system prompts

1. Log on to the Wave Server via Windows Remote Desktop using a valid Wave administrator user name and password.
2. Click **Start > Run**.
3. Launch the Global Administrator Management Console via the following command:

   ```
   “C:\Program Files\Artisoft\TeleVantage
   Administrator\TVAdmin.exe” /sentence
   ```
4. Start the User/Group Management applet using the `/sentence` command line option.
5. Choose **Tools > Test Sentences**. The Test Sentences dialog opens.



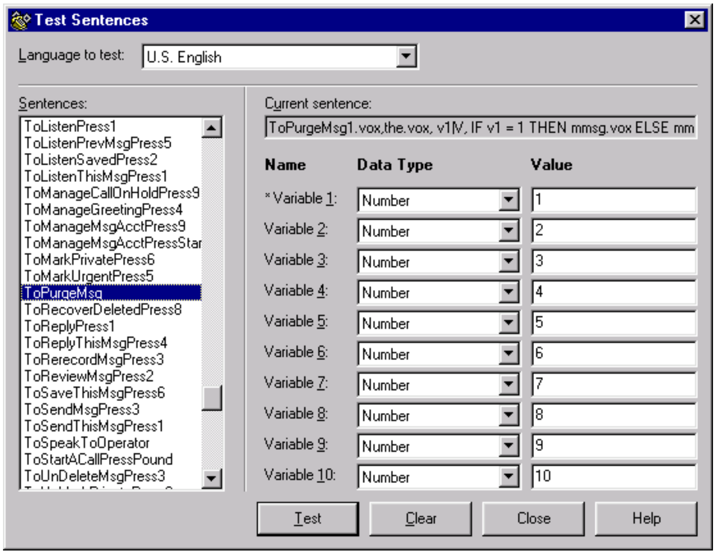
Language to test: U.S. English

Current sentence: GreetActive.vox,v1\V

Name	Data Type	Value
* Variable 1:	Number	1
Variable 2:	Number	2
Variable 3:	Number	3
Variable 4:	Number	4
Variable 5:	Number	5
Variable 6:	Number	6
Variable 7:	Number	7
Variable 8:	Number	8
Variable 9:	Number	9
Variable 10:	Number	10

6 In **Language to test**, select the language of the prompts that you want to test.

7 Under **Sentences**, select a sentence from the list.



Test Sentences

Language to test: U.S. English

Sentences:
ToListenPress1
ToListenPrevMsgPress5
ToListenSavedPress2
ToListenThisMsgPress1
ToManageCallOnHoldPress9
ToManageGreetingPress4
ToManageMsgAcctPress9
ToManageMsgAcctPressStar
ToMarkPrivatePress6
ToMarkUrgentPress5
ToPurgeMsg
ToRecoverDeletedPress8
ToReplyPress1
ToReplyThisMsgPress4
ToRerecordMsgPress3
ToReviewMsgPress2
ToSaveThisMsgPress6
ToSendMsgPress3
ToSendThisMsgPress1
ToSpeakToOperator
ToStartACallPressPound
ToUnDeleteMsgPress3

Current sentence: ToPurgeMsg1.vox,the.vox, v1|V, IF v1 = 1 THEN mmsg.vox ELSE mm

Name	Data Type	Value
*Variable 1:	Number	1
Variable 2:	Number	2
Variable 3:	Number	3
Variable 4:	Number	4
Variable 5:	Number	5
Variable 6:	Number	6
Variable 7:	Number	7
Variable 8:	Number	8
Variable 9:	Number	9
Variable 10:	Number	10

The **Current sentence** box displays how that sentence is described in the sentences.ini file. Many sentences consist of a single WAV file. Other sentences are made up of several joined WAV files, and may contain variables as well.

8 You can double click a sentence to test it, or select it and press **Test.** When your phone rings, pick it up and listen to the sentence in the language you selected. You can continue to play messages, and even change languages, without hanging up your phone.

9 If the sentence contains variables, they are indicated in the **Name** column with an asterisk. You can enter a new **Value** for a variable, and optionally select a different variable **Data Type**.

For example, by default the sentence ToPurgeMsg sentence plays as:

> "To permanently delete the 1 message in your ViewPoint's Deleted folder, press 3. Otherwise, press 4."

By changing the **Value** of Variable 1 to 6, the sentence plays as:

> "To permanently delete the 6 messages in your ViewPoint's Deleted folder, press 3. Otherwise, press 4."

Click **Clear** to return all **Values** to their original settings.

Chapter 19

Recording All Wave Calls

Chapter Contents

Wave can automatically record all calls handled by the system, while exempting the individuals, roles, or queues of your choice. For example, you could record all calls except for those belonging to users in the Administrators role. You can also exempt internal (station-to-station) calls, and tandem (trunk-to-trunk) calls.

System call recordings are stored in a voice mailbox of your choice. You can manage them exactly as you would manage voice messages. For instructions on how to play and manage voice messages using the phone or ViewPoint, or how to manage archived recordings using the Wave Archived Recording Browser, see Appendix A of *Wave ViewPoint User Guide*.

Note: Users can also record their own calls manually—see the *Wave ViewPoint User Guide*, and you can configure Contact Center queues to automatically record calls (see the *Wave Contact Center Administrator Guide*).

Privacy issues with call recording

Caution! *It is the license-holder’s responsibility to comply with any federal, state, or other applicable statutes regarding the recording of phone calls. Vertical Communications, Inc. disclaims any responsibility for failing to comply with such regulations.*

Some countries, states, or other locations require that you announce to callers that their calls may be or are being recorded.

- Wave includes a system prompt, MayBeMonitored.wav, that says, “Your call may be monitored or recorded,” which you can play as needed (for example, by using an auto attendant or Contact Center queue greeting).
- Wave allows you to play a regular “reminder beep” while recording Contact Center queue calls which alerts agents and callers that their calls are being recorded (see “Including a reminder beep on queue call recordings” on page 19-10).

Important! Be sure to instruct any users with the Wave permission “Record calls” (or who inherit this permission from a role) how to comply with call recording privacy requirements.

Disk space and recording all calls

Caution! *If you record all calls or even a significant portion of calls, or if you have users with thousands of saved voice messages and large maximum mailbox sizes, disk space on the Wave Server can quickly fill up with voice messages and call recordings. In addition, ViewPoint performance will significantly degrade while a user searches for and acts on thousands of recordings, or when recordings are being delivered to the user in quick succession.*

See “Determining where to store call recordings” on page 19-4 for best-practice information on how to manage many recordings.

What parts of the call are recorded

Call recordings include only calls with two or more parties, and only the portion of the call from the time the parties are connected to the end of the call.

The following parts of a call are NOT recorded:

- Hold music
- Auto attendant messages
- Voicemail greetings
- Voicemail messages
- Phone commands or prompts
- IVR Plug-in prompts
- Consultation calls during supervised transfers

When a call is transferred, the various conversations are included in a single call recording.

Exempting Contact Center queue calls from system call recording

Contact Center queues usually comprise a large portion of a system's total phone traffic. If your site uses Contact Center queues, it is recommended that you exempt your queues from system call recording, and use the queue's own recording features to record queue calls. Otherwise, needless duplication of recordings can result.

- You exempt queue calls from system call recording as described in step 10 in the "Recording all calls" procedure starting on page 19-8.
- For information about queue call recording, see "Automatically recording queue calls" in Chapter 2 in the *Wave Contact Center Administrator Guide*.

Preparing to record all calls

Before starting to record all calls, plan carefully so that you allocate adequate system resources and avoid impacting system performance.

Recording all Wave calls can use significant amounts of disk space and can consume many Call Record resources. Before beginning to record calls, you should plan for how to store the resulting voice files and manage the demand for Call Record resources.

See the following topics for more information:

- “Disk space and recording all calls” on page 19-2.
- “Determining where to store call recordings” on page 19-4.
- “Allocating DSP resources for call recordings” on page 19-7.

Determining where to store call recordings

You can store your call recordings on the Wave Server, or offload them to another location.

- **Offloading call recordings:** Each minute of call recording consumes .46 MB of disk space. If you store all call recordings on the Wave Server, these files can rapidly consume your available hard disk space and interfere with phone system performance and users’ ability to receive voice messages. Therefore, it is highly recommended that you automatically offload call recordings from the Wave Server.

  For two ways to do so, see “Offloading call recording voice files from your Wave Server” on page 19-5.
- **Storing call recordings on the Wave Server:** see “Storing call recordings on the Wave Server” on page 19-7 for information on how to limit the amount of space consumed by call recordings by automatically making room for the newest call recordings by deleting the oldest ones.

Offloading call recording voice files from your Wave Server

If you want to offload call recording files from your Wave Server, you have two options:

- Automatic archiving. See page 19-5.
- Sending call recordings to a e-mail address. See page 19-5.

Automatically archiving recordings

To save space on the Wave Server and improve ViewPoint performance, you can archive call recordings to another location. The recommended approach to archiving is to have Wave automatically archive all recordings of a certain age. You can choose which users are subject to automatic archiving and you can specify the network location of your choice for archive files. Recordings are archived in WAV or MP3 format with detailed Call Log information about each call.

Once call recordings are archived, users with permission can then search, manage and listen to the archived recordings using the Wave Archived Recording Browser. See “Archiving call recordings and voicemail” on page 22-24.

Sending recordings to any e-mail address

As an alternative to automatic archiving, you can use Wave e-mail notification to automatically send call recordings to any e-mail address. To do so:

1. Create a placeholder user (named, for example, “Recorded Calls”) to whom you send all call recordings.
2. Set up e-mail notification for the user with the following selections:
   - **Send e-mail for all messages**
   - **Attach voice message and delete from Inbox**

   For instructions on setting up e-mail notification, see “Setting e-mail notification” on page 11-44.

With these settings, the call recording files are moved to your e-mail server in the form of e-mail attachments, with detailed Call Log information, and are deleted from the Wave Server as soon as they arrive, so that no extra disk space is consumed.

When you offload call recording files via e-mail notification, you will have a large number of e-mails in the e-mail account to which they are sent—one e-mail for each recorded call. Wave automatically puts information about the call into the e-mail's subject and body, so that you can use your e-mail program's Search capability to find a particular call recording. The e-mail's subject holds information in the following format:

```
SysRec: TrunkX/NAME->Station Y/User Y
```

where `->` indicates the direction of the call, `Trunk X` indicates the trunk number involved and the Caller ID name (where available), `Station Y` indicates the station ID of the station involved, and `User Y` indicates the extension of the user involved.

The e-mail body also includes the following Call Log information that further describes what was recorded (example data used):

```
Notes:
Trunk 1/ Unknown -> Station 2/ Queue 500

CustomData:
CustProp1=Value of Custom Property 1;CustProp2=Value of
Custom Property 2;

--- Call Recording Details ---
Direction: Inbound
From: Unknown
To: Queue 500
Answered By: User 2
From Number: 6172344500
To Number: 500
From Code: <None>
To Code: <None>
From Device: Trunk 1
To Device: Station 2
Duration: 01:07
Start Time: 8/31/2005 11:17:55
Stop Time: 8/31/2005 11:19:02
Wait Time: 00:07
Parties: 2
Caller ID Name: <None>
Organization: <None>
Call Log ID: 04010000002119

Wave Code:1207:1010:1
```

Storing call recordings on the Wave Server

If you decide to store call recordings on the Wave Server instead of offloading them, you should choose the amount of disk space that you want to devote to storing call recording files. Even if you configure Wave to automatically archive call recordings daily you still need enough disk space to hold 24 hours of recordings before they are archived. When this space is filled, you can have Wave automatically make room for the newest call recordings by deleting the oldest.

To automatically make room for new call recordings

1. Limit the size of the placeholder user’s voice mailbox to the amount of disk space you want to devote to call recordings. Use the formula 1 minute = .46MB. For example, to devote 1 GB to call recordings, set the user’s voice mailbox to 2185 minutes. See “Configuring the user’s voice mailbox” on page 11-29.
2. Configure system call recording to automatically delete the oldest call recording when the mailbox is full. See “Recording all calls” on page 19-8.

Allocating DSP resources for call recordings

Before beginning to record all calls, make sure that your system configuration includes enough DSP resources to meet the increased demand.

System call recording uses Call Record resources, and optionally SIP Gateway resources. (You allocate these resources via the Resource Management applet, as described in “Using the Resource Management applet and Resource Management Advisor” on page 23-45.) See:

- How many Call Record resources do I need? See page 19-8.
- When do I need SIP Gateway resources? See page 19-8.

Note: Playing reminder beeps during Contact Center queue call recording does not require that you allocate any DSP resources. This is a change from previous versions, which required one Prompt Assist resource which was shared by all queue calls that were being recorded.

How many Call Record resources do I need?

- **Two Call Record resources are required for each user-to-user call recording session.** When recording conference calls, no additional Call Record resources are needed, no matter how many parties are in the call.
- **The number of Call Record resources to allocate depends on the number of simultaneous call recordings that Wave needs to support.** In general, the number of Call Record resources assigned should be double the maximum number of simultaneous calls that the system needs to record. If a call comes in and resources are not available to record the call, the call will proceed as normal but will not be recorded.
- **A typical application of call recording is to record all external calls and exclude internal station-to-station calls.** In this scenario, a good rule of thumb is to allocate double the number of Call Record resources as there are working trunks on the system. For example, allocating 20 Call Record resources will fully support recording all external calls for 10 trunks.

When do I need SIP Gateway resources?

If call recording involves a SIP end point (either a SIP trunk or SIP station), one IP Gateway resource is required for each SIP endpoint.

When recording conference calls, one IP Gateway resource is required for each SIP call leg.

Recording all calls

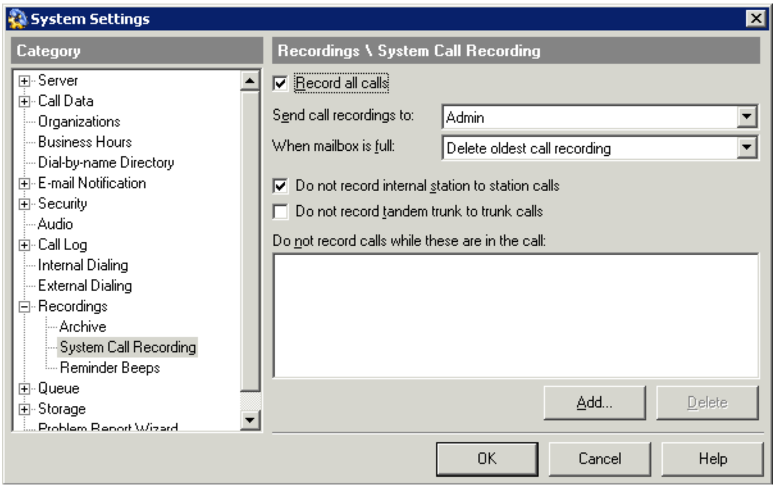
Use the following procedure to set up the automatic recording of all Wave calls, and specify exemptions for calls that you do not want to record:

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the User/Group Management icon, located in the PBX Administration section of the Management Console.
3. Choose **Tools > System Settings**. The System Settings dialog opens.

4 Click the Recordings \ System Call Recording tab.



☑ Record all calls

Send call recordings to: Admin

When mailbox is full: Delete oldest call recording

☑ Do not record internal station to station calls

☐ Do not record tandem trunk to trunk calls

Do not record calls while these are in the call:

5 Select the **Record all calls** checkbox to have Wave automatically record system calls according to the settings you specify in this dialog. If not selected, Wave does not record system calls.

Note: If this checkbox is not selected, users can still record their own calls manually, and Contact Center queues can still automatically record all queue calls.

6 From the **Send call recordings to** drop-down list, select the voice mailbox to which system call recordings are sent.

7 From the **When mailbox is full** drop-down list, choose one of the following options:

- **Discard new call recording**. Wave deletes the new call recording instead of storing it. When this option is selected, call recording stops when the target mailbox is full.
- **Delete oldest call recording**. Wave automatically deletes the oldest call recording in the mailbox to make room for the new recording. Only call recordings will be automatically deleted, never voice messages.

8 Select the **Do not record internal station to station calls** checkbox to exempt internal calls from system call recording. If not selected, the system records internal station-to-station calls as well as inbound and outbound calls that involved a trunk.

9 Select the **Do not record tandem trunk to trunk calls** checkbox to exempt tandem calls (inbound calls to Wave that are routed to external phone numbers) from system call recording. If not selected, the system records tandem trunk-to-trunk calls as well as inbound and outbound calls that involved a trunk.

For more about tandem call routing, “Tandem call routing” on page 29-22.

10 Use the **Do not record calls while these are in the call** list to exempt users or roles from system call recording. You can exempt any of the following entities:

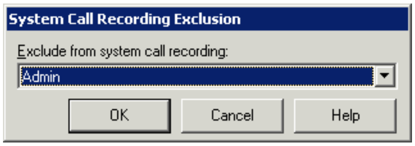
- **Users**. Wave does not record any call while an exempted user is a participant.

  If an exempted user joins a conference call that is being recorded, recording pauses as long as the exempted user is in the call. If the exempted user leaves the conference, recording resumes.

- **Roles**. Wave does not record any call while a member of the exempted role is a participant.

- **Queues**. Wave does not record any Contact Center queue call. Note that when a queue call is transferred to a user who is not an agent in the queue, it ceases being a queue call and call recording will begin if none of the other exemptions apply.

Click **Add** to exempt a user, role, or queue to the list. The System Call Recording Exclusion dialog opens Select a user, role, or queue from the drop-down list, then click **OK**.



System Call Recording Exclusion

Exclude from system call recording: Admin

Click **Delete** to delete the selected user, role, or queue from the list.

11 When you are finished adding exemptions, click **OK**.

Including a reminder beep on queue call recordings

You can include a regular “reminder” beep on Contact Center queue call recordings. If enabled, a short tone is played to all parties in the call and is audible in the recording.

Note: Including a beep on *user* or *system* call recording is not supported in this version

See “Allocating DSP resources for call recordings” on page 19-7 for information about system resource requirements and reminder beeps:

To include a reminder beep on queue call recordings

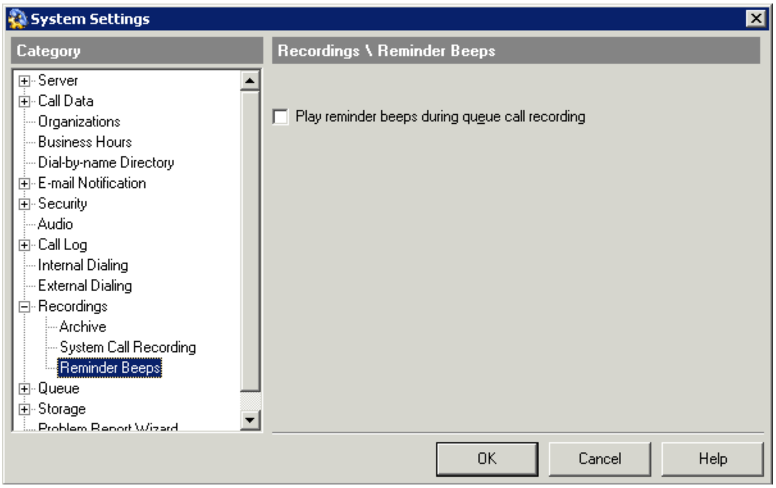
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Click the Recordings \ Reminder Beeps tab.



□ Play reminder beeps during queue call recording

5 Select the **Play reminder beeps during queue call recording** checkbox to play reminder beeps during automatic call recording of Contact Center queue calls, including both queue call recordings and agent call recordings.

6 Click **OK**.

Archiving call recordings

To save space on the Wave Server and improve ViewPoint performance, you can archive call recordings to a location of your choice. Users can then search for and manage archived recordings using the Wave Archived Recording Browser. See “Archiving call recordings and voicemail” on page 22-24.

Chapter 20

Tracking and Distinguishing Calls

Chapter Contents

Wave provides several ways to track groups of similar calls for purposes of record-keeping, billing, or automated call handling.

The most basic way to track related calls is by sorting the Call Log (see “Using the Call Log view” on page 22-5), and by running reports using the Wave Contact Center Reporter. For information about basic Contact Center Reporter reports available on all Wave systems, see Chapter 13 in the *Wave ViewPoint User Guide*. For information about the complete suite of reports available to licensed Contact Center installations, see Appendix A in the *Wave Contact Center Administrator Guide*.

This chapter describes the following more advanced methods of tracking and distinguishing calls:

- **Using Organizations**. Organizations enable two or more separate businesses or contractors to share a Wave Server and trunks, yet be independent of each other in terms of caller experience and internal billing. See page 20-2.
- **Using account codes**. With user-entered account codes you can distinguish any group of calls for reporting and accounting purposes. For example, if your office contains employees or contractors whom you bill separately for their phone use, you can use account codes to mark calls by the user they belong to. Other uses of account codes include marketing campaigns, case and issue tracking, and more. See page 20-10.
- **Using custom data variables**. Custom data variables enable you to attach information to incoming calls, for example, the name of the product that the caller is calling about. Users can view custom data variables in their Call Monitors, and you can set up automatic call handling based on custom data values. You can also report on calls involving custom data variables. See page 20-18.

Using Organizations

With Organizations, multiple separate businesses or other groups can share a Wave Server, yet remain independent. Callers dialing a user in one Organization will never know that other businesses exist on the same phone system, and internal billing can be kept strictly separate.

Once you have defined Organizations and assigned each user to the appropriate Organization, you can do the following:

- Log calls by Organization for purposes of tracking or billing.
- Restrict callers at the auto attendant from dialing extensions of users in other Organizations than the one that they called.
- Distribute outbound trunk use between Organizations.
- Display a call’s Organization in the ViewPoint Call Monitor.

This section covers the following aspects of using Organizations:

- “How calls are logged by Organization” on page 20-2
- “Creating and populating an Organization” on page 20-3
- “Creating an auto attendant for each Organization” on page 20-9.
- “Configuring Operators for multiple Organizations” on page 20-9.

How calls are logged by Organization

For each call that is associated with an Organization, the Organization name appears in the Organization column in the Call Log:

- Outbound calls display the Organization of the user who placed the call.
- Inbound calls display the Organization of the user who answered the call (the **Answered By** user.)
- Conference calls display the Organization of the user who initiated the conference.

Creating and populating an Organization

You can create an Organization and add users in either of the following ways:

- **Via the Organizations applet** as described below. When you use this method, you can create an Organization and also assign all of its members at the same time.
- **Via the User/Group Management applet** as described on page 20-6. When you use this method, after creating the Organization, you must edit each user individually to assign that user to the Organization.

Once you have created an Organization, you can add users at a later time using either method.

Note: A user can belong to only one organization. Also, users in different Organizations cannot have identical extensions—even if they belong to different organizations, each Wave user must still have a unique extension.

Creating and populating an Organization via the Organizations applet

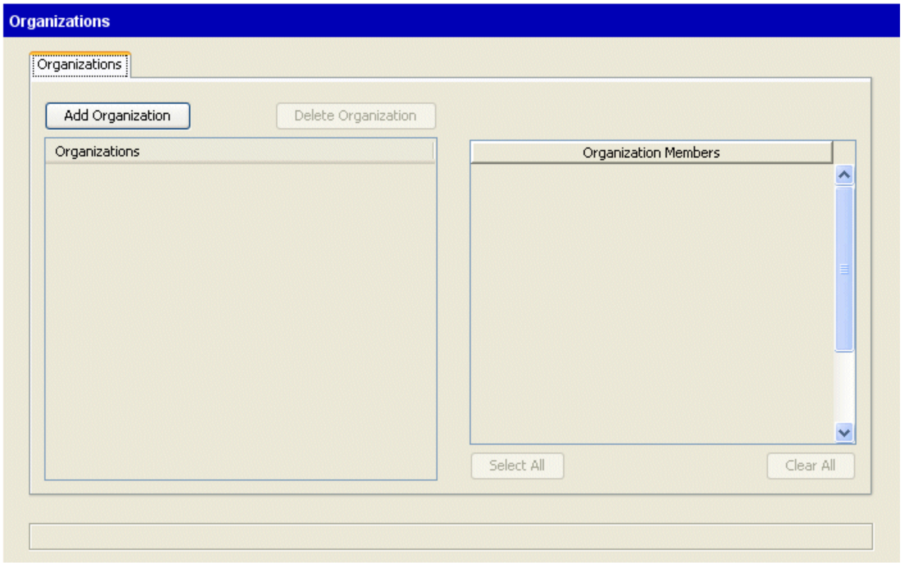
To define an Organization via the Organizations applet

1 If necessary, click the Administration tab of the Management Console.

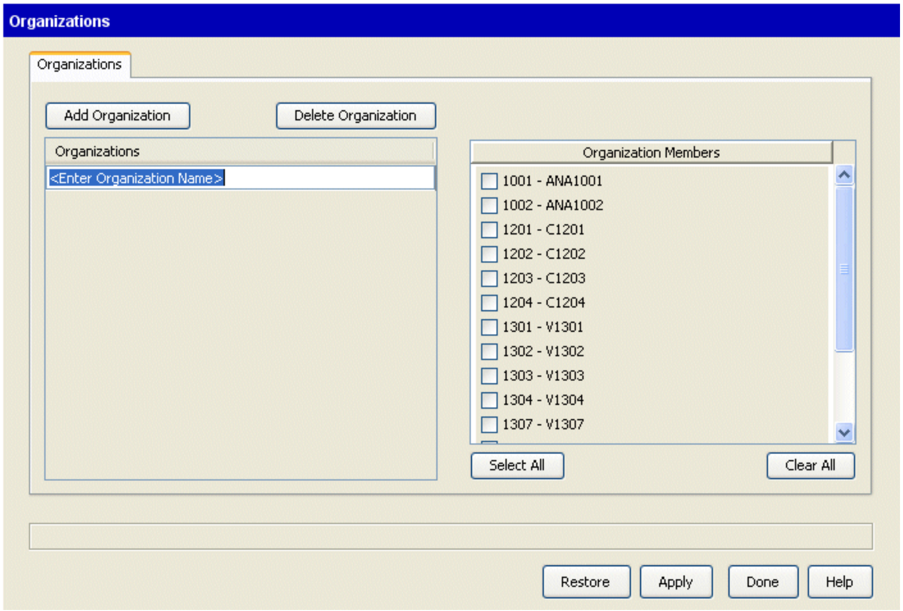
Click

2 Click the Organizations icon, located in the PBX Administration section of the Management Console.

3 The Organizations dialog opens.



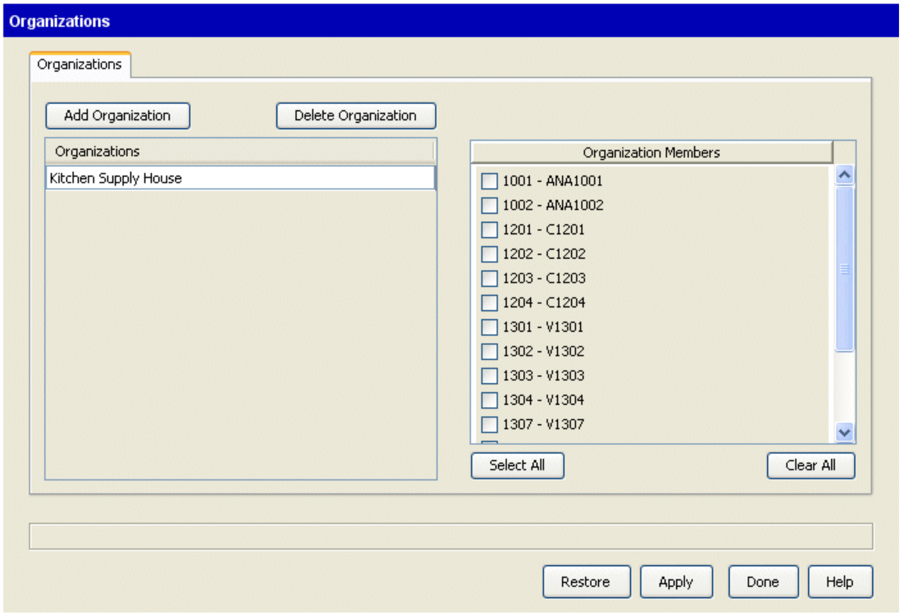
4 Click **Add Organization**.



<Enter Organization Name>

□ 1001 - ANA1001
□ 1002 - ANA1002
□ 1201 - C1201
□ 1202 - C1202
□ 1203 - C1203
□ 1204 - C1204
□ 1301 - V1301
□ 1302 - V1302
□ 1303 - V1303
□ 1304 - V1304
□ 1307 - V1307

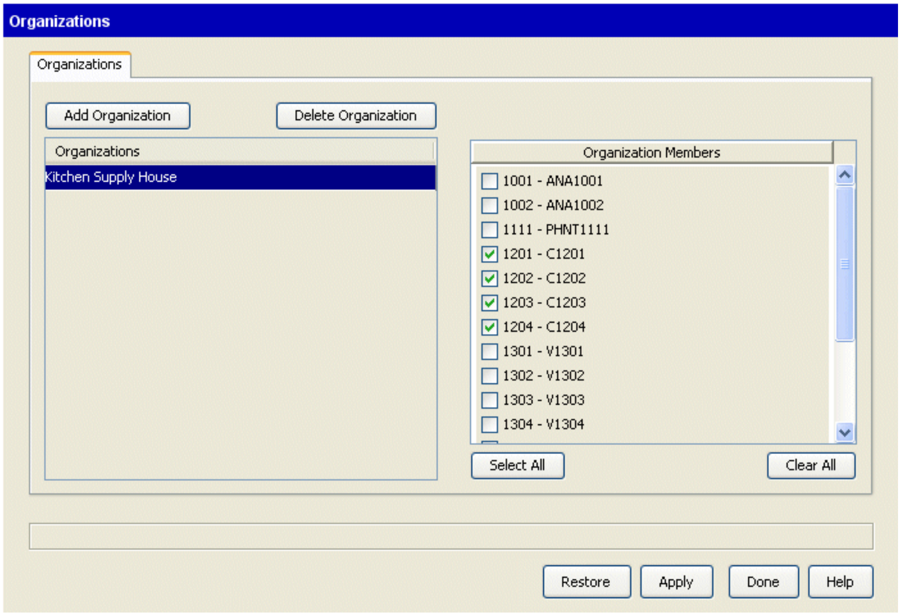
5 Enter a name for the new Organization.



Kitchen Supply House

□ 1001 - ANA1001
□ 1002 - ANA1002
□ 1201 - C1201
□ 1202 - C1202
□ 1203 - C1203
□ 1204 - C1204
□ 1301 - V1301
□ 1302 - V1302
□ 1303 - V1303
□ 1304 - V1304
□ 1307 - V1307

6 To add members to the organization, click the Organization name.



Organizations

Organizations

Add Organization Delete Organization

Organizations
Kitchen Supply House

Organization Members
□ 1001 - ANA1001
□ 1002 - ANA1002
□ 1111 - PHNT1111
☑ 1201 - C1201
☑ 1202 - C1202
☑ 1203 - C1203
☑ 1204 - C1204
□ 1301 - V1301
□ 1302 - V1302
□ 1303 - V1303
□ 1304 - V1304

7 In the right pane, select one or more user’s checkbox to add the user to the Organization. Deselect a user’s checkbox to remove the user from the Organization.

8 Click **Apply** (to save your changes and continue working) or **Done** (to save your changes and close the Organizations applet.)

Creating and populating an Organization via the User/Group Management applet

To create an Organization via the User/Group management applet

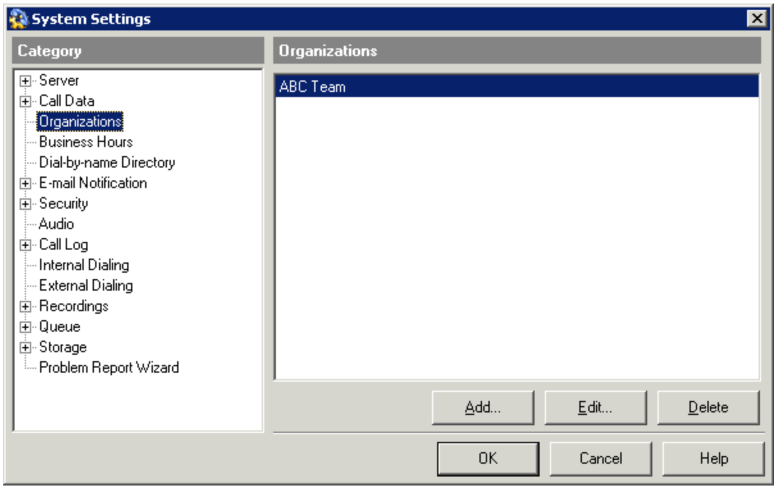
1 If necessary, click the Administration tab of the Management Console.

Click

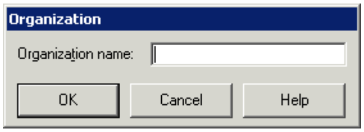
2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the Organizations tab, which lists the Organizations you have defined so far.



5 To add a new Organization, click **Add**. The Organization dialog opens.



6 Enter the name of the Organization, for example, the name of the company that is sharing the Wave Server.

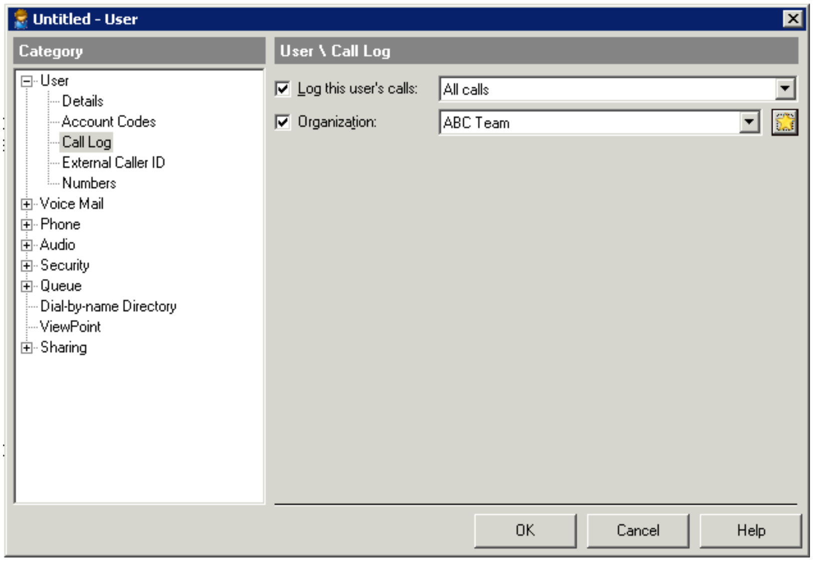
7 Click **OK** to return to the Organizations dialog.

8 When you are done adding Organizations, click **OK** to close the System Settings dialog.

To assign a user to an Organization via the User/Group management applet

1 In the Users view, double-click the user to open the User dialog, and choose the User \ Call Log tab.

2 Select the **Organization** checkbox and then select the Organization to which the user should belong. Click ☆ to create a new Organization.



☑ Log this user's calls: All calls

☑ Organization: ABC Team

See “Creating and populating an Organization via the Organizations applet” on page 20-3.

3 Click **OK**.

Note: If a Contact Center queue agent is configured to place calls as the queue, the agent’s Organization is still displayed for the call, not the queue’s Organization.

Creating an auto attendant for each Organization

You can define a separate auto attendant for each Organization, if each Organization has its own phone number. Callers will hear a greeting and menu choices specific to the Organization that they are calling, and they will be unable to accidentally dial users in other Organizations, either by extension or via the dial-by-name directory.

To create an auto attendant for an Organization

1 Create a public ViewPoint Group containing the same users that are the members of the Organization. For instructions see “Creating a ViewPoint Group” on page 12-5.

2 Define an auto attendant as described in “Configuring an auto attendant” on page 13-3. Check **Restrict dial-by-name and extension matching to members of** on the Menu Choices tab, and select the ViewPoint Group.

3 Route the trunk(s) corresponding to the Organization’s phone number to the auto attendant. To associate a DID number with an auto attendant, edit the appropriate Trunk Groups entry via the Trunk Configuration applet, and map the DID number to the auto attendant’s extension.

Configuring Operators for multiple Organizations

At several places in the Wave system, callers can press 0 to transfer to an Operator. With multiple Organizations, you might want to have a different Operator for each Organization. To set up multiple Operators and make sure that callers reach the right Operator for the Organization they are calling, do the following:

1 Decide which extensions will be the Operators for the different Organizations. For example, 101 for Company ABC, and 102 for company YYZ. These examples are used in the following steps.

2 Edit each user. On the User \ Details tab use the **Operator** field to select the Operator extension appropriate to the user’s Organization. For example, if a user belongs to Organization ABC, select extension 101. This ensures that callers pressing 0 while leaving a user voicemail are handled correctly.

For full instructions, see “The User \ Details tab” on page 11-19.

3 If you are using Wave Contact Center queues, edit each queue. On the General tab under **Operator**, select the extension appropriate to the queue’s Organization. For example, if the queue belongs to Organization ABC, select extension 101. This ensures that callers pressing 0 while leaving the queue voicemail are handled correctly.

See the *Wave Contact Center Administrator Guide* for complete information on creating and using a Contact Center.

Using account codes

With Wave, you can track your phone traffic by either optionally allowing or requiring users to enter an account code for each call. Account codes can represent any aspect of your phone traffic that you want to track—customer number, product line, department, and so forth. You define the available account codes and tell your users the codes that they should or must enter under specific circumstances.

Some of the ways you can use account codes include:

- **Billing clients**. With account codes you can track calls to various customers whom you bill for the phone time you spend with them. You can associate account codes with contacts for automatic customer tracking.
- **Internal accounting**. If phone bills are a significant part of your company’s expenses, you can use account codes to perform detailed expense analyses. For example, you can track phone use by department.

- **Marketing campaigns**. By setting up an account code for the campaign and having agents use it whenever they place or receive campaign calls, you can track the time, resources, and results of the campaign.

For example, your legal office is working on the Gould case and the Avellanos case. You assign the Gould case an account code of 88 and the Avellanos case an account code of 55. Whenever users place or receive calls that relate to the Gould case, they enter 88. Whenever they place or receive calls relating to the Avellanos case, they enter 55. You can then run a Call Log report that sorts calls by account code and see the phone traffic for the Gould and Avellanos cases separately. (You can also run a report that sorts by user, so that you can see how much phone time a specific user spent on each case.)

See the following topics for more information:

- Available user account code modes. See page 20-11.
- How users enter account codes. See page 20-12.
- How the end of an account code is detected. See page 20-13.
- Viewing account code information in the Call Log or Call Monitor. See page 20-13.
- Reporting on account code information. See page 20-14.
- Setting system-wide account code options. See page 20-14.
- Setting a user’s account code modes. See page 20-16.
- Creating a valid account code list. See page 20-16.
- Using the verbal account code prompt instead of a beep. See page 20-18.

Available user account code modes

In the current version, you specify whether account code entry is optional or required on a per-user basis. A user’s account code mode can be different for inbound vs. outbound calls. With some modes, the value entered by a user is checked against a list of valid codes.

The following user account code modes are available:

- **Optional non-verified**. Do not prompt the user to enter account codes on outbound calls. If the user enters an account code, accept it without verification.
- **Optional verified**. Do not prompt the user to enter account codes on outbound calls. If the user enters an account code, verify it.

- **Forced non-verified - All calls**. Prompt the user to enter an account code on all outbound calls, if one has not already been entered. Accept the account code without verification.
- **Force verified - All calls**. Prompt the user to enter account code on all outbound calls, if one has not already been entered, and verify it.
- **Forced non-verified - Long distance calls only.** Prompt the user to enter an account code on all outbound long-distance calls, if one has not already been entered. Accept the account code without verification.
- **Force verified - Long distance calls only.** Prompt the user to enter account code on all outbound long-distance calls, if one has not already been entered, and verify it. See "Creating a valid account code list" on page 20-16 for details on how to create the account code list used when a user is assigned the account code mode **Optional verified** or **Forced verified.**

How users enter account codes

You should tell users what account codes to enter and in which circumstances. Users can enter account codes in the following ways:

- **When prompted to do so after placing an outbound call**. Only users forced to enter account codes will hear this prompt.

  By default the account code prompt is a beep. To change it, see "Using the verbal account code prompt instead of a beep" on page 20-18.
- **After a call has finished**. In ViewPoint, a user can enter an account code for a completed call by selecting the call in the Call Log and choosing **Actions > Enter account code**. The user must have the Wave permission **Access Call Log folder** set to "View and Edit" (see "Wave permissions" on page 11-127).

How the end of an account code is detected

When users use the phone to specify an account code, Wave detects the end of the account code when any of the following occurs:

- The account code reaches the maximum number of digits. To define the maximum number of digits, see “Setting system-wide account code options” on page 20-14.
- The user presses #.
- Three seconds elapse after the user entered a digit. The system assumes that the digits already entered are the account code that the user intended to enter.

If a user does not enter an account code before 5 seconds have elapsed after the beep or prompt, the system beeps or prompts the user to enter the account code again.

Note: If you have a high maximum number of digits and your account codes can be of variable lengths, you should encourage phone users to press **#** when they reach the end of an account code.

Users can cancel an account code entry while they are entering it by pressing *****.

Viewing account code information in the Call Log or Call Monitor

The Call Log view contains an Account Code column that shows the account code associated with each call. If the Account Code column is blank, no account code was entered for the call. Click the Account Code column header to sort the Call Log by account code. For more information, see “Using the Call Log view” on page 22-5.

Note: In the Call Log, you can change a call’s account code or enter a new one. Select the call and choose **Call Log > Enter Account Code**.

ViewPoint’s Call Monitor view also contains an Account Code column, but it is hidden by default. In the Call Monitor view, choose **View > Show Columns** to display it.

Reporting on account code information

You can view call activity by account code by generating the Call Log report using the Wave Contact Center Reporter. For information about basic Contact Center Reporter reports available on all Wave systems, see Chapter 13 in the *Wave ViewPoint User Guide*. For information about the complete suite of reports available to licensed Contact Center installations, see Appendix A in the *Wave Contact Center Administrator Guide*.

You can also export the Call Log, with its account code information, to a CSV file that you can then view in spreadsheet or reporting applications. Note that you can only export the Call Log as an administrator via User/Group Management, as described in “Exporting the Call Log” on page 22-14. You cannot export a user’s Call Log from ViewPoint.

Setting system-wide account code options

Before setting up account code modes for individual users, you should configure the system-wide account code options as follows:

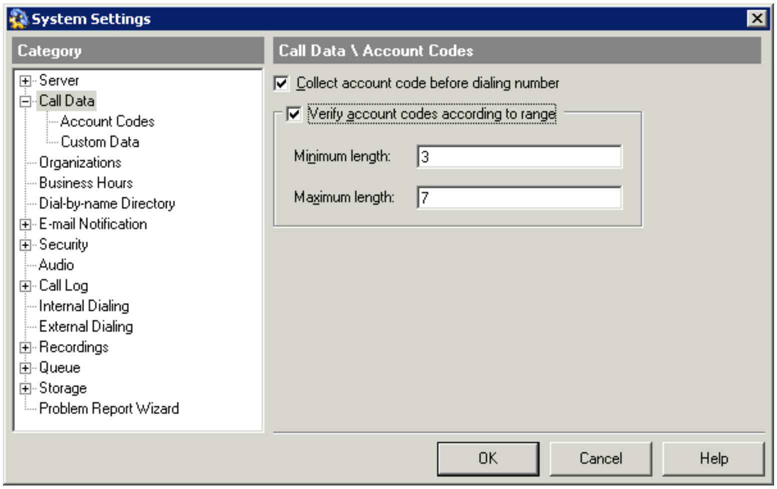
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the Call Data \ Account Codes tab.



☑ Collect account code before dialing number

☑ Verify account codes according to range

Minimum length: 3

Maximum length: 7

5 Select the **Collect account code before dialing number** checkbox to prompt for an account code after the user dials an access code (for example, 9).

6 Select the **Verify account codes according to range** checkbox to have the system verify that an account code contains the correct number of digits. If the account code entered contains too many digits or too few digits, a user is prompted to enter it again.

Specify the **Minimum length** and **Maximum length** to be used for validation. For example, if account codes in your system can be two, three, or four digits, enter a **Minimum length** of 2 and a **Maximum length** of 4.

Note: It is more efficient to set **Minimum length** and **Maximum length** to the same number and use account codes that are all the same length. When set up this way, the system immediately recognizes when users finish entering an account code, so they do not need to press **#** at the end of the account code. When account codes are of variable length, users must press **#** to end the account code or there will be a slight pause while the system waits for more digits.

If **Minimum length** and **Maximum length** are both set to 0, account codes will not be verified by length.

7 Click **OK**.

Displaying account codes for contacts in the ViewPoint Call Monitor

On an incoming call from a ViewPoint contact, Wave can automatically display the contact's account code information along with the call in the ViewPoint Call Monitor.

This system-wide option is disabled by default. In this version, you enable this option via a registry setting. To do so:

1 Add the following DWORD registry setting:

```
HKLM\Software\Artisoft\TeleVantage\Server\Settings\
SetAccountCodeFromContact
```

2 Set the registry setting to 1. The setting will take effect the next time the Wave Server is restarted.

Setting a user’s account code modes

On a per-user basis, you can specify whether account code entry is optional or required. A user’s account code mode can be different for inbound vs. outbound calls. For details, see “The User \ Account Codes tab” on page 11-21.

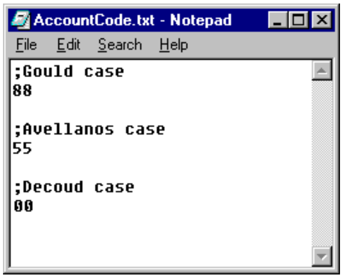
Creating a valid account code list

If you want to verify account codes for some or all users, you must first create a text file that lists all of your valid account codes. When a user whose account code mode requires verification enters an account code, Wave checks the account code against the contents of the text file. If the account code is not listed in the text file, Wave prompts the user to re-enter it.

The text file must be called `Accountcode.txt` and it must reside in the \Accountcode directory on the Wave Server computer. The default location is:

```
C:\Program Files\Artisoft\TeleVantage Server\Accountcode\
Accountcode.txt
```

Use a text editor such as Notepad to create and maintain the account code file.



```
;Gould case
88

;Avellanos case
55

;Decoud case
00
```

Note the following:

- Enter each account code as a separate line in the text file.
- Blank lines are ignored, and can make the list easier to view and maintain.
- Comment lines are ignored, and must start with a semicolon (;).
- Account codes can contain numbers, letters, and other characters. However, only ViewPoint users can enter numbers and other characters via the keyboard. If you have users who will only enter account codes using the phone, be sure to use numeric-only account codes.

- The account codes that you enter in the text file must meet the minimum and maximum account code range that you specified or they will be ignored. For example, if you specified that account codes must be between 2 and 4 digits, a 5-digit account code will be ignored even if it is displayed in the text file. See “Setting system-wide account code options” on page 20-14 for instructions on setting account code length requirements. (
- You can use the wild card characters ? and % when you enter account codes in the text file:
    - **Question mark (?)**. Indicates any single digit. For example, an account code entry of 12? would make 123, 124, and 129 all valid account codes. In this case, however, neither 12 nor 1233 would be valid account codes.
    - **Percent sign (%)**. Indicates any number of digits, including none. For example, an account code entry of 12% would make 12, 123, 1233, and 12789213120 all valid account codes.

If you use *either* wild card character in an account code, it must be the final character in an account code, and if you use *both* wild card characters in the same account code, the % character must be the final character.

Valid	Invalid
12?	1?2
12??	1%2
12%	?12
12?%	%12
12?????%	12%?

Note that account codes that are identical *except* for wild card characters will conflict with each other. For example, 1234 conflicts with 1234? and 1234%. In the case of conflicting entries, only the first entry in the text file is used to verify account codes.

Using the verbal account code prompt instead of a beep

By default, the account code prompt is a single beep. You should explain to your users that they must enter an account code when they hear the beep. Wave provides an alternate account code sound file, a verbal prompt that says, “Please enter an account code.”

To use the verbal account code prompt instead of the beep

1. Find the file `AccountCodePrompt.wav` in the user directory. This file contains the beep. The default location is:

   ```
   C:\Program Files\Artisoft\TeleVantage Server\VFiles\
   AccountCodePrompt.wav
   ```

2. Rename the file, for example, to `AccountCodePrompt.wav.beep`.

Users now hear the verbal prompt instead of the beep when they are prompted to enter an account code.

Note: By renaming the beep file, Wave automatically uses another AccountCodePrompt.wav file, which is found in your language directory and which contains the verbal prompt. The default path for the English language verbal prompt file is the following. It (or any other language version of this file) can be rerecorded using the System Prompts view.

```
C:\Program Files\Artisoft\TeleVantage Server\VFiles\EN00\
AccountCodePrompt.wav
```

Using custom data variables

Wave lets you attach extra information to incoming calls, using *custom data variables*. The information is displayed to users in ViewPoint’s Call Monitor, and can also be used to automate call handling. For example, based on the caller’s auto attendant choice, set a variable called Product to the name of the product that the caller is calling about. For example, callers who press 1 have Product=“Widget,” while callers who press 2 have Product=“Advanced Widget.” When users answer the calls they see the product name in the Call Monitor in a column labeled “Product.”

Note: Custom data variables are case sensitive.

Using custom data variables is a two-step process:

1 Defining a custom data variable (see page 20-19.)

2 Setting the value for a custom data variable (see page 20-21.)

Defining a custom data variable

You can define as many custom data variables as you want.

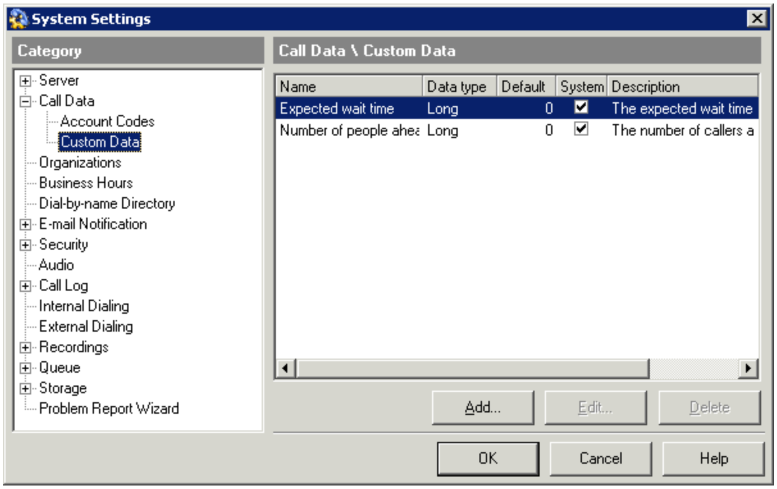
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

1 Choose **Tools > System Settings**. The System Settings dialog opens.

2 Choose the Call Data \ Custom Data tab, which lists the custom data variables created so far.

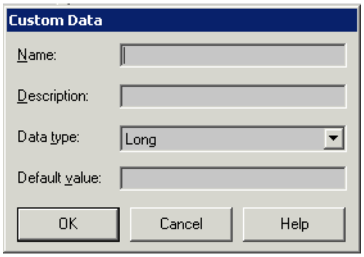


Name	Data type	Default	System	Description
Expected wait time	Long	0	☑	The expected wait time
Number of people ahea	Long	0	☑	The number of callers a

Each custom data variable is attached to every incoming call, though a given variable might not be used for every call.

Note: If you have purchased the Wave Call Center module, two system variables are present by default, Expected wait time and Number of people ahead. For instructions on using them, see the *Wave Contact Center Administrator Guide*.

3 To create a new custom data variable, click **Add**. The Custom Data dialog opens.



Custom Data

Name:

Description:

Data type: Long

Default value:

4 Enter the following information for the custom data variable:

- **Name**. Enter a name for the variable. Keep the name relatively short, as it will appear in a column header in the ViewPoint Call Monitor. Custom data variable names are case sensitive.
- **Description**. Enter a description that helps you remember how the variable is used.
- **Data Type**. This field determines the type of information that the variable holds. Select one of the following from the drop-down list:
  - **Long**. Variable holds integer numbers only.
  - **Double**. Variable can hold integer numbers or decimal point numbers.
  - **Boolean**. Value must be either 0 or 1.
  - **String**. Variable holds text. Text variables are sorted alphabetically. For example, you can have a Hold prompt play if a variable is in the “range” from A to E. In that case, any text string beginning with A, B, C, D, or E would cause the prompt to play. Note that numbers can be part of a text string, but they are treated as text characters.
- **Default value**. Enter the value that the variable assumes if no other action sets a value. For example, if callers are prompted to enter their Customer Priority Numbers to set this variable, and a caller chooses not to enter the data, you can have the variable default to a low-level Customer Priority Number. For string variables you can leave the field blank, indicating that the variable is empty by default. For numeric variables you must enter a number, usually 0.

5 Click **OK** to add the custom data variable to the list.

6 Click **OK** to close the System Settings dialog.

The variable you created is now available to be attached to any incoming call (for example, by an auto attendant or Contact Center queue). Users have a corresponding column in the Call Monitor where they can view the variable’s value for each call.

Setting the value for a custom data variable

You can have Wave set the value of a custom data variable in the following ways:

- **Auto attendant menu choice**. When defining an auto attendant menu choice, you can have it set the value of one or more custom data variables. See “Defining menu choices” on page 13-6.
- **Contact Center queue**. You can have a queue set the value of a custom data variable based on caller data entry. See the *Wave Contact Center Administrator Guide*.
- **IVR Plug-in**. An IVR Plug-in can set the value of custom data variables based on a variety of methods, including when it was called and caller data entry. For more information see Appendix G of the *Wave Server Installation Guide*.
- **Wave Call Classifier**. The Wave Call Classifier can set custom data variables based on database queries, Caller ID name or number, account codes, or other custom variables.

Advanced Data Networking Configuration

CHAPTER CONTENTS

Caution! *The settings described in this chapter are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

Configuring dial-up routing

When configuring dial-up routing, you will typically configure the parameters only once, when you install and configure Vertical Wave the first time. If you change ISP providers or access numbers, you may need to modify these settings.

Configuring dial-up routing requires you to configure demand-dial interfaces. To configure demand-dial interfaces, you must create an entry for *each* remote location (ISP, headquarters, another sales office) to which you want to dial out. The RRAS administrator stores the settings needed to connect to a particular remote router or network in a “phone book entry.” Once an interface is configured in RRAS, it acts like any server.

Note: When configuring an internal modem for dial-out routing, you cannot configure the modem to dial digits following the connection of the call. For example, you cannot configure an internal modem to dial a number, delay, and then dial more digits.

After initial configuration, you will only need to modify these settings if you add remote locations or change phone access numbers.

Typically, you configure dial-up routing for both dial-in and dial-out capabilities. You can configure for only one or the other, and if you do, how you define dial-out properties depends on several things. Various possibilities are described in the following table.

Modem Port Usage	Enables	Wave Variables
Dial out as RAS client	The Wave Server behaving as a dial-up client, calling a server/router. A WAN device will be used for outbound dial-on-demand connections.	This is typically used only for debugging or testing Wave connections, because it creates a client-to-server connection, where Wave is the client—instead of a network-to-network connection.
Receive calls as RAS server	Outside clients (non-network- connected users) calling into Wave. WAN devices will be used for inbound dial-on-demand connections.	If you have a T-1 data line to the Internet, you could select this option for one WAN device to provide remote access for employees.
Dial out and receive calls as a demand-dial router	The Wave Server calling an ISP (a network-to-network connection from one router to another). WAN devices will be used for inbound and outbound dial-on-demand connections.	If you have a T-1 data line to the Internet, you could select this option for any WAN device.

Caution! *When connecting two Wave Servers together using ISDN, set the network side of the connection to the linear hunt type and the user side to the reverse linear hunt type. For more information about GLARE, see “Minimizing Glare” on page 27-7.*

Configuring network services and routing protocols

The following sections describe how to configure network services and routing protocols on the Wave Server.

- "Configuring network routing protocols" on page 21-3
- "Configuring the Wave Server as a network services client" on page 21-6
- "Configuring DHCP relays" on page 21-9
- "Setting up static routes" on page 21-10

Configuring network routing protocols

By default, the routing protocols described in the following topics are installed but not configured on the Wave Server, as they are not typically required for most configurations.

- "Configuring routing information protocol (RIP)" on page 21-3
- "Configuring the open shortest path first (OSPF) routing protocol" on page 21-5

Configuring routing information protocol (RIP)

Hint: If you are using RIP with multiple connection lines and want line speed taken into account during routing, modify routing protocol metrics accordingly when configuring an interface or when adding a static route.

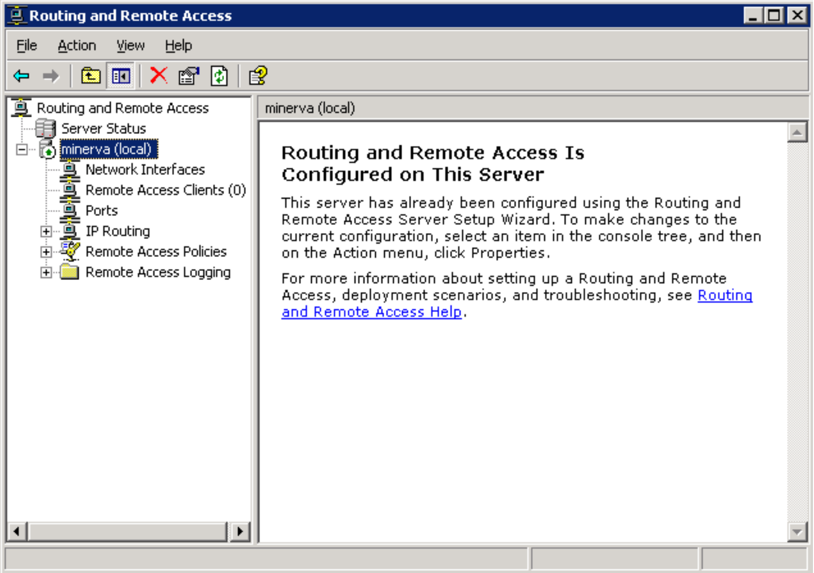
Note: Unlike making network settings changes, when using RRAS, your changes will take effect immediately; the Wave Server will not restart.

To configure RIP

Click

1 Open the Microsoft RRAS applet under Data Administration on the General Administration tab of the Management Console. Log on using your Wave username and password. The Routing and Remote Access dialog opens.

For more information about logging in with a remote connection, see “Remote access applets” on page 2-7.



Routing and Remote Access

Routing and Remote Access Is Configured on This Server

This server has already been configured using the Routing and Remote Access Server Setup Wizard. To make changes to the current configuration, select an item in the console tree, and then on the Action menu, click Properties.

For more information about setting up a Routing and Remote Access, deployment scenarios, and troubleshooting, see Routing and Remote Access Help.

2 Add the RIP protocol.

Right-click the General folder under IP Routing, and choose **New Routing Protocol**. In the New Routing Protocol dialog, click **RIP Version 2 for Internet Protocol** and click **OK**.

3 Select each interface on which you want to enable the routing protocol.

Right-click RIP in the IP Routing folder and select **New Interface**. Select the desired interface, then click **OK**. Configure the Internet properties for that interface on the dialog that opens, then click **OK**.

4 Close the Routing and Remote Access dialog to return to the Management Console.

Note: If you are routing across a WAN, be sure to configure the WAN interface on the Integrated Services Card with RIP. Auto-static, static, and default routing can be used with demand-dial interfaces. Auto-static makes static routing table entries, and is used only for demand-dial connections, and only with other Wave Servers or with a remote Microsoft Windows server acting as a router. Periodic polling will keep a line up all the time, and should be used only with persistent connections.

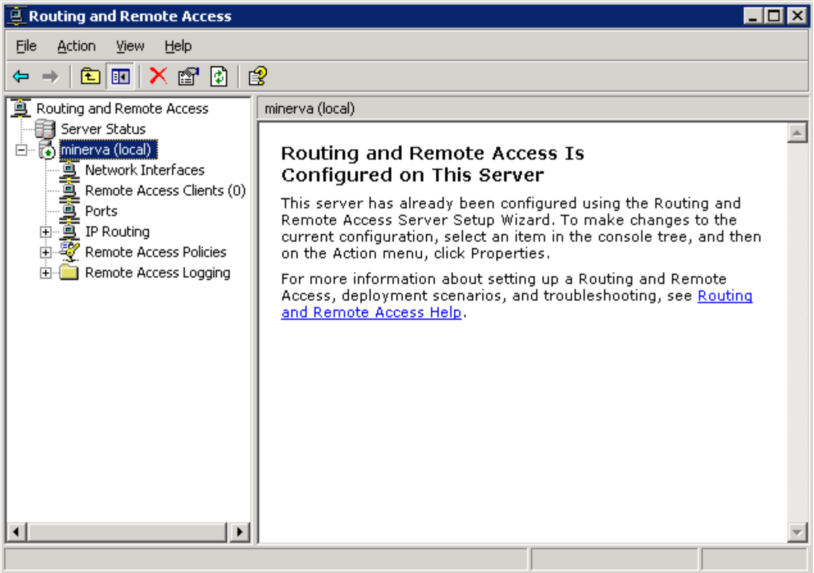
Configuring the open shortest path first (OSPF) routing protocol

To configure OSPF

Click

1 Start the Microsoft RRAS applet under Data Administration on the General Administration tab of the Management Console. Log on using your Wave username and password. The Routing and Remote Access dialog opens.

For more information about logging in with a remote connection, see “Remote access applets” on page 2-7.



Routing and Remote Access Is Configured on This Server

This server has already been configured using the Routing and Remote Access Server Setup Wizard. To make changes to the current configuration, select an item in the console tree, and then on the Action menu, click Properties.

For more information about setting up a Routing and Remote Access, deployment scenarios, and troubleshooting, see Routing and Remote Access Help.

2 Add the OSPF protocol.

Right-click the General folder under IP Routing, and choose **New Routing Protocol**. In the New Routing Protocol dialog, click “Open Shortest Path First (OSPF)” and click **OK**.

3 Select each interface on which you want to enable the routing protocol.

Right-click OSPF in the IP Routing folder and select **New Interface**. Select the desired interface, then click **OK**. Configure the Internet properties for that interface on the dialog that opens, then click **OK**.

Note: If the interface you want to add is not shown in the Select Interface dialog, add it to the Summary by choosing Add Routing Protocol from the Actions menu.

4 Close the Routing and Remote Access dialog to return to the Management Console.

Configuring the Wave Server as a network services client

The Wave Server cannot be a client to a DHCP server, as each Wave LAN network interface/routing port must use a static IP address.

Refer to the following topics for detailed information:

- Configuring the Wave Server as a DNS client
- Configuring the Wave Server as a WINS client
- IP addressing

Configuring the Wave Server as a DNS client

Note: Make sure the Wave Server has a valid static IP address.

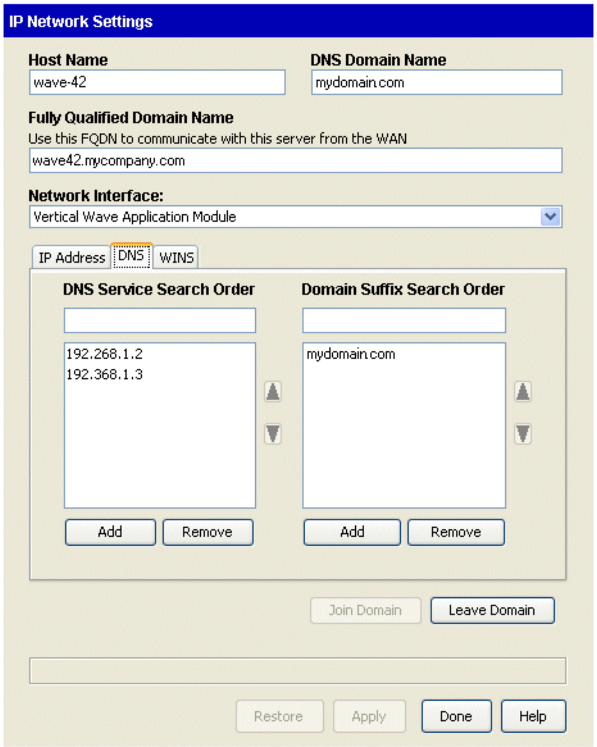
To configure your Wave Server as a DNS client

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Network Settings icon, located in the Data Administration section.

3 Click the DNS tab.



IP Network Settings

Host Name: wave-42

DNS Domain Name: mydomain.com

Fully Qualified Domain Name
Use this FQDN to communicate with this server from the WAN
wave42.mycompany.com

Network Interface: Vertical Wave Application Module

DNS Service Search Order:
192.268.1.2
192.368.1.3

Domain Suffix Search Order:
mydomain.com

4 Enter the IP address of your DNS server (the server that resolves DNS name queries) in the **DNS Service Search Order** field, then click **Add**.

The order in the list is the order in which they will be queried. Put the IP address of the preferred DNS server first. Typically, the local company's DNS server should be first.

If the list contains addresses, you can use the arrows to move the IP addresses up and down to change the search order.

If you need to remove the DNS server, select the address in the list and click **Remove**.

You can add additional DNS servers to the list for redundant or additional name resolution services.

5 Enter the domain suffix in the **Domain Suffix Search Order** field.

If the list contains domain suffixes, you can use the arrows to move the them up and down to change the search order.

You can add additional domains to the list.

6 Click **Apply** to confirm your changes. Changes take effect after you reboot your Wave Server.

Configuring the Wave Server as a WINS client

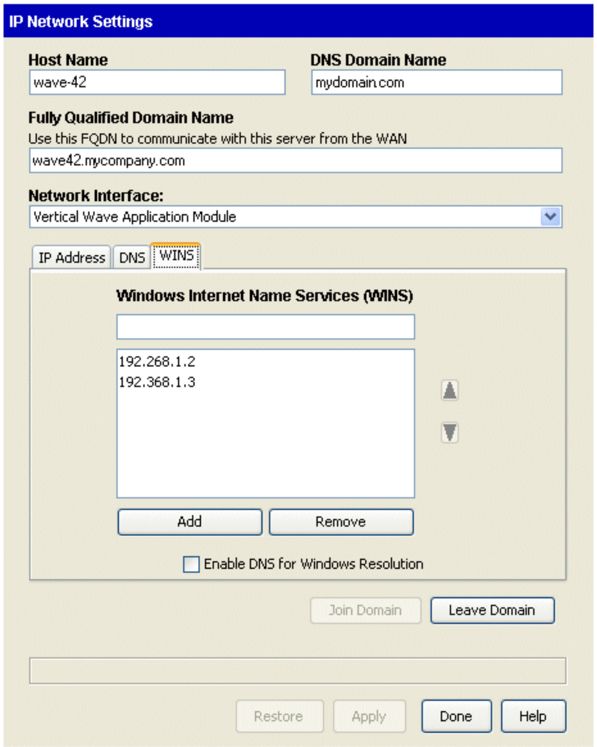
To configure your Wave Server as a WINS client

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Network Settings icon, located in the Data Administration section.

3 Select the WINS tab.



IP Network Settings

Host Name: wave-42

DNS Domain Name: mydomain.com

Fully Qualified Domain Name
Use this FQDN to communicate with this server from the WAN
wave42.mycompany.com

Network Interface: Vertical Wave Application Module

Windows Internet Name Services (WINS)

192.268.1.2
192.368.1.3

□ Enable DNS for Windows Resolution

4 Select a network interface from the **Network Interface** drop-down list.

Setting up each network interface as a WINS client is recommended.

5 Enter the appropriate server address in the **Windows Internet Name Services (WINS)** field, and click Add.

Wave registers its name and IP address with the primary WINS server.

6 Select the **Enable DNS for Windows Resolution** checkbox if the Wave Server will also be a DNS client. This option ensures that DNS servers are also used to resolve client requests.

Note: When DNS is enabled here, you also need to enter DNS server information on the DNS tab of the IP Network Settings applet.

7 Repeat steps 4 through 6 to configure each interface.

8 Click **Apply** to confirm your changes. Changes take effect after your Wave Server is rebooted.

Configuring DHCP relays

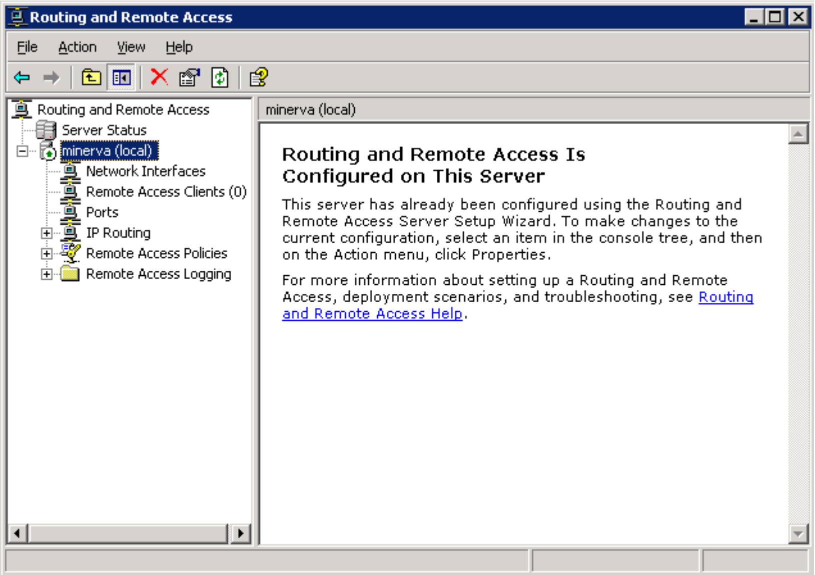
Note: Before starting this procedure, ensure you have the IP address of your DHCP server.

To enable and configure a DHCP relay agent

Click

1 Open the Microsoft RRAS administration tool, and log on using your Wave username and password.

For more information about logging in with a remote connection, see “Remote access applets” on page 2-7.



Routing and Remote Access Is Configured on This Server

This server has already been configured using the Routing and Remote Access Server Setup Wizard. To make changes to the current configuration, select an item in the console tree, and then on the Action menu, click Properties.

For more information about setting up a Routing and Remote Access, deployment scenarios, and troubleshooting, see Routing and Remote Access Help.

2 Right-click DHCP Relay Agent in the IP Routing folder and select **New Interface**.

3 Select the desired interface and click **OK**.

4 Click **OK** to return to the Management Console.

Setting up static routes

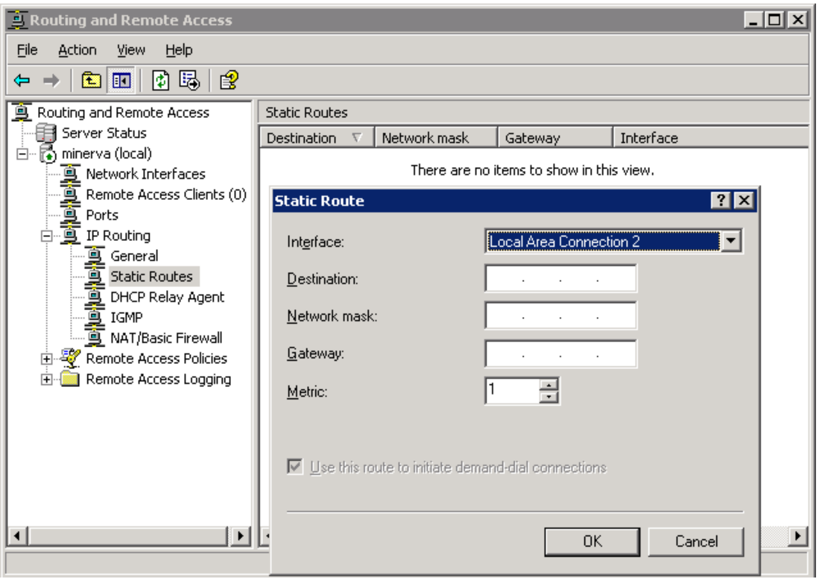
To set static routes

Click

1 Start the Microsoft RRAS administration tool, and log on using your Wave username and password.

For more information about logging in with a remote connection, see “Remote access applets” on page 2-7.

2 Right-click Static Routes in the IP Routing folder, and choose **New Static Route**. The Static Route dialog opens.



There are no items to show in this view.

Interface: Local Area Connection 2

Destination: . . .

Network mask: . . .

Gateway: . . .

Metric: 1

☑ Use this route to initiate demand-dial connections

3 Select an **Interface** from the drop-down list.

4 Type a **Destination** IP address, subnet **Network mask**, **Gateway**, and **Metric**.

5 Click **OK**.

6 Close the Routing and Remote Access dialog to return to the Management Console.

Note: When you are configuring for a demand-dial modem connection, you must create a static route for each modem connection to the ISP/headquarters because it is not part of a larger network. If you know the IP address of a remote office, you can put it in the static routing table. You will typically create a default static route (IP address `0.0.0.0`, subnet `0.0.0.0`, and an appropriate gateway address) to be used as a last resort for packets that Wave does not know where to send. When you are configuring a static route for a digital connection, you must enter the gateway address, which is the IP address for the router on the other side of the digital connection, sometimes called the *far end* or *next hop* router. If you configure a gateway address, you will set up a default static route to that gateway.

Chapter 22

Monitoring and Maintenance

CHAPTER CONTENTS

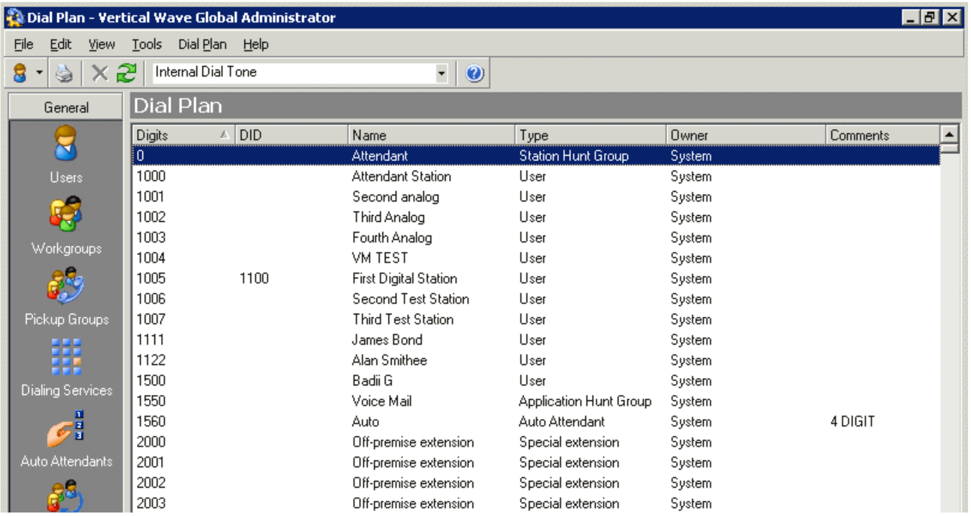
This chapter describes several methods of monitoring and maintaining your Wave system via the User/Group Management applet.

You can also monitor your system using the Wave Contact Center Reporter, which lets you run reports on a variety of system elements, including trunk use, call traffic, queues, agents, identified callers, account code use, and more. For information about basic Contact Center Reporter reports available on all Wave systems, see Chapter 13 in the *Wave ViewPoint User Guide*. For information about the complete suite of reports available to licensed Contact Center installations, see Appendix A in the *Wave Contact Center Administrator Guide*.

Another way to monitor your Wave system is to automatically record all calls for later review. See Chapter 19.

Managing your dial plan with the Dial Plan view

You can view and manage your dial plan as a whole using the Dial Plan view.



Digits	DID	Name	Type	Owner	Comments
0		Attendant	Station Hunt Group	System	
1000		Attendant Station	User	System	
1001		Second analog	User	System	
1002		Third Analog	User	System	
1003		Fourth Analog	User	System	
1004		VM TEST	User	System	
1005	1100	First Digital Station	User	System	
1006		Second Test Station	User	System	
1007		Third Test Station	User	System	
1111		James Bond	User	System	
1122		Alan Smithee	User	System	
1500		Badii G	User	System	
1550		Voice Mail	Application Hunt Group	System	
1560		Auto	Auto Attendant	System	4 DIGIT
2000		Off-premise extension	Special extension	System	
2001		Off-premise extension	Special extension	System	
2002		Off-premise extension	Special extension	System	
2003		Off-premise extension	Special extension	System	

The Dial Plan view shows each number in your system that can be dialed from an internal dial tone, identified by name and type. It lists only numbers beginning with the digits 0-9, and so does not include Wave phone commands such as those beginning with Flash or *. It does include the following:

- All enabled extensions (users, auto attendants, Contact Center queues, and so forth.)
- Users’ contacts dialable by the user's extension + PIN
- User extensions plus * for direct-to-voice-mail dialing, if the feature is enabled (see “Setting general options” on page 4-4)
- Dialing service access codes
- System extensions such as 411 for the dial-by-name directory

You can filter the Dial Plan view using the toolbar drop-down list to show only those numbers that are dialable from external phones (**PSTN**) or SIP servers.

You can use the Dial Plan view to check your dial plan for ambiguous numbers and correct them when they occur.

You can edit a dial plan entry by selecting it and choosing **Dial Plan > Open**. The appropriate dialog for editing that number opens.

Note: If the **Dial Plan > Open** option is unavailable, you may not have permission to access or edit the selected item.

You can delete a dial plan entry using the **Delete** button or the toolbar Delete icon.

Using the Maintenance Log view

The Maintenance Log view displays tracked actions and presents details about each action. Information contained in the log is stored in the database. To open the Maintenance Log view, click its button in the view bar. The Maintenance Log tracks many administrative actions, including:

- Restarting a device
- Starting the Wave Server
- Stopping the Wave Server
- Scheduling a Wave Server shutdown
- Changing a user’s password
- Changing a queue’s password
- Logging on to the User/Group Management applet
- Logging out of the User/Group Management applet
- Account lockout
- Trunk hangup after maximum login attempt
- Changing any editable item in any User/Group Management applet view
- Deleting an item from a view
- Enabling or disabling a device

The following columns appear in the Maintenance Log view:

- Action taken
- Item that was acted upon (if applicable)
- Date and time of the action
- Name of the user who was logged on when the change was made
- Name of the computer from which the change was made
- Details about the action

Navigating the Maintenance Log view

The Maintenance Log view shows 50 entries at a time, in a default order starting with the most recent. You can show the next or previous 50 entries by choosing **Maintenance Log > Next 50 entries** or **Maintenance Log > Next 50 entries.**

You can also jump to a particular date by choosing **Maintenance Log > Jump to date**. Enter the date in the dialog that opens and click **OK**.

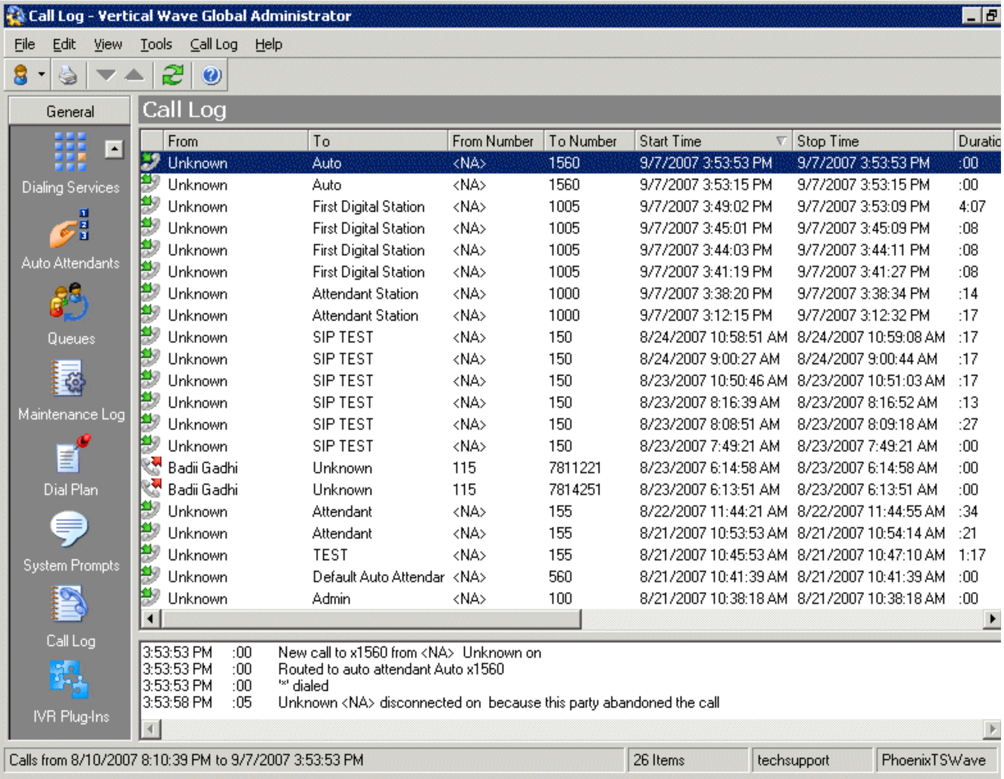
Clearing the Maintenance Log

To clear the Maintenance Log, click ☑ in the toolbar.

Using the Call Log view

The Call Log view displays a record of the calls placed and received on the Wave system. Each call is displayed as a row in the view. You can use the Call Log view to analyze system usage patterns, and you can export Call Log records to generate traffic analysis reports.

To open the Call Log view, click its button in the view bar.



Call Log

From	To	From Number	To Number	Start Time	Stop Time	Duratio
Unknown	Auto	<NA>	1560	9/7/2007 3:53:53 PM	9/7/2007 3:53:53 PM	:00
Unknown	Auto	<NA>	1560	9/7/2007 3:53:15 PM	9/7/2007 3:53:15 PM	:00
Unknown	First Digital Station	<NA>	1005	9/7/2007 3:49:02 PM	9/7/2007 3:53:09 PM	4:07
Unknown	First Digital Station	<NA>	1005	9/7/2007 3:45:01 PM	9/7/2007 3:45:09 PM	:08
Unknown	First Digital Station	<NA>	1005	9/7/2007 3:44:03 PM	9/7/2007 3:44:11 PM	:08
Unknown	First Digital Station	<NA>	1005	9/7/2007 3:41:19 PM	9/7/2007 3:41:27 PM	:08
Unknown	Attendant Station	<NA>	1000	9/7/2007 3:38:20 PM	9/7/2007 3:38:34 PM	:14
Unknown	Attendant Station	<NA>	1000	9/7/2007 3:12:15 PM	9/7/2007 3:12:32 PM	:17
Unknown	SIP TEST	<NA>	150	8/24/2007 10:58:51 AM	8/24/2007 10:59:08 AM	:17
Unknown	SIP TEST	<NA>	150	8/24/2007 9:00:27 AM	8/24/2007 9:00:44 AM	:17
Unknown	SIP TEST	<NA>	150	8/23/2007 10:50:46 AM	8/23/2007 10:51:03 AM	:17
Unknown	SIP TEST	<NA>	150	8/23/2007 8:16:39 AM	8/23/2007 8:16:52 AM	:13
Unknown	SIP TEST	<NA>	150	8/23/2007 8:08:51 AM	8/23/2007 8:09:18 AM	:27
Unknown	SIP TEST	<NA>	150	8/23/2007 7:49:21 AM	8/23/2007 7:49:21 AM	:00
Badii Gadhi	Unknown	115	7811221	8/23/2007 6:14:58 AM	8/23/2007 6:14:58 AM	:00
Badii Gadhi	Unknown	115	7814251	8/23/2007 6:13:51 AM	8/23/2007 6:13:51 AM	:00
Unknown	Attendant	<NA>	155	8/22/2007 11:44:21 AM	8/22/2007 11:44:55 AM	:34
Unknown	Attendant	<NA>	155	8/21/2007 10:53:53 AM	8/21/2007 10:54:14 AM	:21
Unknown	TEST	<NA>	155	8/21/2007 10:45:53 AM	8/21/2007 10:47:10 AM	1:17
Unknown	Default Auto Attendar	<NA>	560	8/21/2007 10:41:39 AM	8/21/2007 10:41:39 AM	:00
Unknown	Admin	<NA>	100	8/21/2007 10:38:18 AM	8/21/2007 10:38:18 AM	:00

```
3:53:53 PM   :00   New call to x1560 from <NA>  Unknown on
3:53:53 PM   :00   Routed to auto attendant Auto x1560
3:53:53 PM   :00   '*' dialed
3:53:58 PM   :05   Unknown <NA> disconnected on  because this party abandoned the call
```

Calls from 8/10/2007 8:10:39 PM to 9/7/2007 3:53:53 PM | 26 Items | techsupport | PhoenixTSWave

Call Log columns

The following table shows the information that is displayed for each call. Several columns are hidden by default. To show and hide columns, right-click the columns header and choose **Columns**.

Column	Description
From	Name of the person who placed the call. On incoming calls, “Unknown” is displayed unless the user identified the caller as a contact. On outgoing calls, this column contains the user’s name.
To	Name of the party who received the call. On incoming calls, the user’s name is displayed. On outgoing calls, “Unknown” is displayed unless the user identified the person as a contact.
Answered By	Name of the user who answered an incoming call or was last dialed. On unanswered calls, the name of the user who was dialed. On answered calls that were subsequently transferred, the name of the transfer recipient, whether or not they answered.
Number	On incoming calls, Caller ID name and number if available. On outgoing calls, the number the user dialed. On a call to or from another Wave user, this field contains <NA>.
From Number	On incoming calls, the caller’s extension or external phone number. On outgoing calls, the user’s extension.
To Number	On incoming calls, the user’s extension or, if the user called into Wave externally, the external number. On outgoing calls, the external number or extension the user called.
Callback Number	If a caller enters a callback number, it is displayed with the prefix “Callback:”
Called Number	On incoming calls, your Direct Inward Dial (DID) number if the caller used it to call you. The field is blank for incoming calls without DID. On outgoing calls, the number you dialed.
Start Time	Date and time that the call started.
Wait Time	On incoming calls, the length of time between dialing the user’s extension and the call being answered. On outgoing calls, Wait Time is always 00:00.
Duration	Length of time that the parties are connected.
Call ID	The Wave ID number of the call. The call ID number also is displayed in queue logs to identify the call (see Appendix A of the *Wave Contact Center Administrator Guide*).

Column	Description
Result	How the caller's wait ended. The assigned values for the possible outcomes are: **Abandoned**. Caller hung up before call was answered. **Connected**. Caller was connected to a party. **To voicemail**. Caller went to voicemail, but did not necessarily leave a message. **Blind transfer**. A blind transfer sent the caller to another party. **Supervised transfer**. A supervised transfer sent the caller to another party. **Login**. Caller logged in to a valid Wave user account. **No Answer**. Outbound call that was not answered. **Login failed**. The caller attempted to log in to a Wave account, but failed to enter a valid password for the maximum number of retries (see “Enforcing strong password security” on page 4-14). **Unknown**. Wave was unable to identify the outcome of the call.
Account Code	The account code entered for the call, if any.
Message	If checked, the caller left a voice message.
Recorded by User	If checked, this call was recorded by a user who handled it.
Recorded by Queue	If checked, this call was automatically recorded by a Contact Center queue.
From Device	On incoming calls, the trunk or extension from which the call originated. On outgoing calls, the user’s station number.
To Device	On incoming calls, the user’s station number. On outgoing calls, the trunk used for the call. If an incoming call was transferred, this column shows the last station that took the call.
Parties	Number of people who took part in the call, including the caller, the called party, anyone to whom the call was transferred, and any conference call participants.
Dial String	Digits that Wave actually dialed over the trunk, which may be different than the digits Wave displays in a contact's phone number. For example, a dial string may contain an international or long-distance access code, a dialing prefix, or a dialing suffix.
From Type	Type of incoming call: Phone or Internet.
From Code	Access code of the dialing service that will be used to return this call. Only applicable to calls coming in from remote Wave Servers over an Internet trunk.
From Rules	If checked, Wave's routing rules will be applied when returning this call.
To Type	Type of outgoing call: Phone, Centrex, or Internet.
To Code	Access code used to dial an outbound call.

Column	Description
To Rules	If checked, routing rules were used to make an outbound call.
Organization	Organization associated with the call, if any. Organizations are associated with outbound calls only, and represent the Organization to which the calling party belongs. For more information see “Using Organizations” on page 20-2.
Custom Data	Custom data, if any, associated with the call.

Copying a Call Log entry

Choosing **Edit > Copy** with a Call Log entry selected copies that Call Log entry as text, including call history.

Viewing a call’s history

When you select a call in the Call Log, its history in the system is displayed in the History pane below. The History pane shows the complete “cradle-to-grave” record of the call from the moment it entered the Wave system until it was disconnected. You can see how a call was routed or transferred, and how it ended.

By default call history data is automatically purged from the system after 5 days to conserve disk space. To adjust the number of days, see “Setting Call Log options” on page 22-9.

Setting Call Log options

You can choose whether to log calls, and which type of calls are logged in the Call Log. To do so:

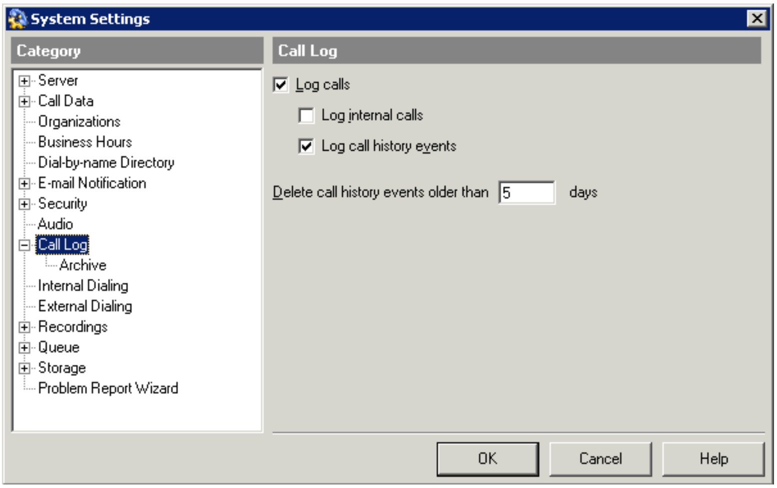
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the Call Log tab.



Call Log

☑ Log calls

☐ Log internal calls

☑ Log call history events

Delete call history events older than 5 days

5 Use the following fields to set up your call logging choices:

- **Log calls**. If checked, Wave logs calls in the Call Log according to the selections you make on this tab. If unchecked, the Call Log is not used.
  - **Log internal calls**. Check to have internal (station-to-station) calls logged in the Call Log. If unchecked, the Call Log only logs calls that involve a trunk.
  - **Log call history events**. Select this checkbox to have call history events logged for recent calls displayed in the Call Log. Note that call history events are purged after a number of days, as defined below.
- **Delete call history events older than __ days**. Enter the number of days that call history text remains in the system before being automatically deleted.

6 Click **OK**.

Displaying a specific number of Call Log entries

The Call Log can become very large over time and its size can cause a delay in its display. To reduce this delay, you can view fewer Call Log items at one time and not load the full database.

To set the number of calls displayed in the Call Log

1 From the User/Group Management applet, choose **Tools > Options**. The Options dialog opens.

2 In **Display __ Call Log entries at a time**, enter the number of entries that you want to appear when you open the Call Log view, using the following as a guide:

- A high setting will likely cause a delay while the specified number of entries are copied over the network, but you can navigate within the information easily using the scrolls bars after the entries have been retrieved.
- A low setting minimizes the delay before information is displayed, but you must retrieve entries more often in order to view the entire Call Log.

3 Click **OK**.

Note: This option controls how many entries are transferred in one request, but does not limit the entries available for view. All Call Log entries are always available by choosing **Call Log > Next 50 Calls** or **Previous 50 Calls**, or using the buttons on the toolbar.

By default, only external calls are logged. For information about logging internal calls, see “Setting Call Log options” on page 22-9. For information about archiving the Call Log, see “Archiving the Call Log” on page 22-11.

Entering an account code for a call via the Call Monitor

To enter an account code for a call or change the one already entered, select the call and choose **Call Log > Enter Account Code**.

Account codes are a means of marking calls for tracking or billing purposes. For more information, see “Using account codes” on page 20-10.

Archiving the Call Log

Over time, Call Log information will begin to fill up your Wave database. To recover database space, you can archive old Call Log information that is no longer needed to a location outside the database.

Caution! *Archived information is permanently removed from the Wave database. You cannot run Contact Center reports on the time period that has been archived.*

Call Log information is written to a comma-separated value (CSV) text file that can be read by most spreadsheet and database applications. The default path is:

```
C:\Program Files\Wave Server\Archive\Calllog.csv
```

You can archive Call Log data in the following ways:

- Set up automatic archiving, which takes place at 1:00 a.m. every day.
- Automatically overwrite the Call Log after a number of days that you specify.
- Perform a manual archive on an as-needed basis, in addition to daily automatic archiving. You can do a manual archive whether or not automatic archiving is turned on.

You do not need to stop the Wave Server or any other Wave components to perform an archive. However, because archiving is database-intensive, you may want to perform it during off-peak hours so that it does not affect normal system operation.

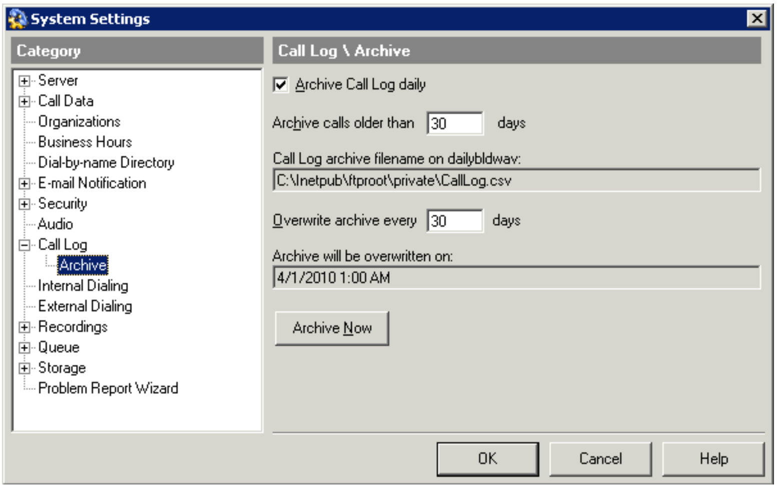
To archive Call Log information

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the User/Group Management icon, located in the PBX Administration section of the Management Console.
3. Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the Call Log \ Archive tab.



☑ Archive Call Log daily

Archive calls older than 30 days

Call Log archive filename on dailybldwav: C:\Inetpub\ftproot\private\CallLog.csv

Overwrite archive every 30 days

Archive will be overwritten on: 4/1/2010 1:00 AM

5 Use the following fields to specify how you want to perform archiving:

- **Archive Call Log daily.** Select this checkbox to automatically archive the Call Log at 1:00 a.m. every day according to the other settings you specify in this dialog. If not selected, the Call Log is written to continually and will increase in size until you manually archive it using the **Archive Now** button described below.
- **Archive calls older than ___ days**. Number of days a call remains in the Call Log until it is archived.
- **Call Log archive file name on <Wave Server name>**. Location and filename of the Call Log archive file on the Wave Server. Call Log archives are written to commas-separated value (CSV) text files that can be viewed with most spreadsheet and database applications.

- **Overwrite archive every ___ days**. Number of days that archived information will be appended to the Call Log archive file. After that number of days, archived information in the file will be deleted and the file will be reused.
- **Archive will be overwritten on**. Date and time that the Call Log archive file will next be overwritten and the data in it deleted. To preserve the archived data, back up the file just before it will be overwritten.

6 Click **Archive Now** to manually archive the Call Log according to the settings specified above. The archive begins immediately and may take several minutes to complete. You can perform a manual archive at any time whether or not automatic archiving is turned on.

Note: You cannot perform any other Global Administrator functions until the archive completes.

7 Click **OK** to save your archiving settings.

Note: Use the Import and Export Wizard (see “Exporting the Call Log” on page 22-14) to create a file containing Call Log information without removing the information from the database.

Exporting the Call Log

You can export the Call Log to a comma-separated value (CSV) file that can be read by most spreadsheet and database applications. Exported Call Log entries are not deleted from the Wave database, and the size of the Wave database does not change after an export.

1. Choose **File > Import and Export**. The Import and Export Wizard opens.
2. Under **Select an import or export action**, select **Export Call Log** and click **Next**.
3. In **Save exported file as**, enter the path and file name for the exported file or click **Browse** to specify a destination.
4. Under **Options**, enter the **Start date** and **End date**.
5. Click **Finish** to export the file. Depending on the size of your Call Log, an export may take several minutes to complete.

Result codes when exporting the Call Log

When the Call Log is exported, the Result field appears as a code. Use the following table to interpret the result codes:

Code	Result
0, 3	Abandoned
1, 2	Connected
4	Left message
5	Blind transfer
6	Supervised transfer
8	Login to phone commands
12	Login failed max number of times

Viewing the Wave Event Log

The Wave Event Log contains a record of all Wave-related system events, including start and stop times of the Wave Server and other Wave applications, and error messages.

Errors indicate that a failure has occurred. Warnings indicate that a critical resource is getting low, though no failures have occurred yet.

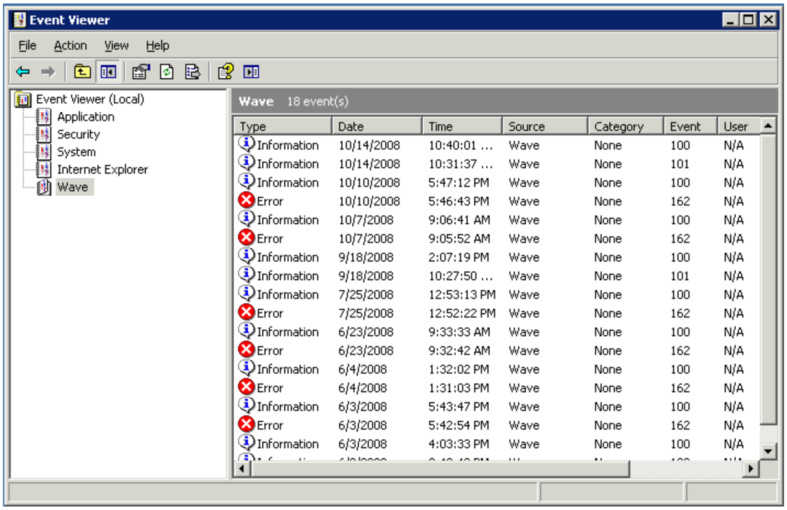
You can set up Wave to send e-mail notifications when events are logged to the Wave Event Log. For more information, see “Setting up Wave Event Log notifications” on page 22-16.

1 If necessary, click the Diagnostics tab of the Management Console.

Click

2 Click the Event Viewer icon.

The Microsoft Management Console - Event Viewer opens:



Wave 18 event(s)

Type	Date	Time	Source	Category	Event	User
Information	10/14/2008	10:40:01 ...	Wave	None	100	N/A
Information	10/14/2008	10:31:37 ...	Wave	None	101	N/A
Information	10/10/2008	5:47:12 PM	Wave	None	100	N/A
Error	10/10/2008	5:46:43 PM	Wave	None	162	N/A
Information	10/7/2008	9:06:41 AM	Wave	None	100	N/A
Error	10/7/2008	9:05:52 AM	Wave	None	162	N/A
Information	9/18/2008	2:07:19 PM	Wave	None	100	N/A
Information	9/18/2008	10:27:50 ...	Wave	None	101	N/A
Information	7/25/2008	12:53:13 PM	Wave	None	100	N/A
Error	7/25/2008	12:52:22 PM	Wave	None	162	N/A
Information	6/23/2008	9:33:33 AM	Wave	None	100	N/A
Error	6/23/2008	9:32:42 AM	Wave	None	162	N/A
Information	6/4/2008	1:32:02 PM	Wave	None	100	N/A
Error	6/4/2008	1:31:03 PM	Wave	None	162	N/A
Information	6/3/2008	5:43:47 PM	Wave	None	100	N/A
Error	6/3/2008	5:42:54 PM	Wave	None	162	N/A
Information	6/3/2008	4:03:33 PM	Wave	None	100	N/A

Setting up Wave Event Log notifications

You can configure Wave to send e-mail notification of each event logged in the Server's Wave Event Log. By setting up notifications, you can stay informed of critical problems, like low disk space, no matter where you are.

To receive e-mail notification of Wave Event Log events

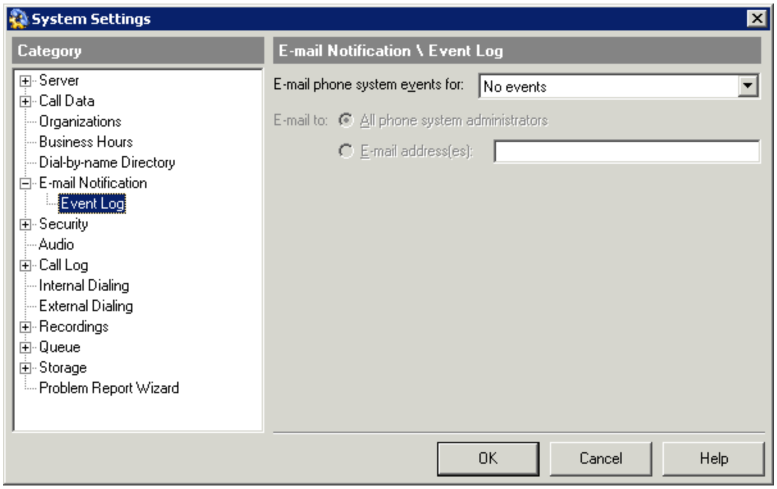
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the E-mail Notification \ Event Log tab.



System Settings

Category

- Server
- Call Data
- Organizations
- Business Hours
- Dial-by-name Directory
- E-mail Notification
  - Event Log
- Security
- Audio
- Call Log
- Internal Dialing
- External Dialing
- Recordings
- Queue
- Storage
- Problem Report Wizard

E-mail Notification \ Event Log

E-mail phone system events for: No events

E-mail to: ● All phone system administrators

○ E-mail address(es):

5 Under **E-mail phone system events for**, select one of the following event levels from the drop-down list:

- **All events**
- **Errors and warnings**
- **Errors only**
- **No events**. No notifications are sent. (This is the default.)

6. Under **E-mail to**, identify to whom the e-mail notifications are sent. (These fields are disabled if you selected **No events**.)
   - **All phone system administrators**. Notifications go to all Wave users with Global Administrator permissions who have e-mail notification turned on. The users you identify here must also have e-mail notification set to receive Windows Event Log notifications (see “Setting e-mail notification” on page 11-44). (This is the default setting.)
   - **E-mail address(es)**. Enter the e-mail addresses of users whom you want to receive notifications, separated by semicolons.
7. Click **OK**.

Wave Event Log messages

The following messages may be posted to the Wave Event Log. Messages are identified in the Wave Event Log by application and message number. Double-click a message in the Event Log to see its text.

This SQL Server has been optimized for 8 concurrent queries. This limit has been exceeded by # queries and performance may be adversely affected.

This event means that occasionally the Wave Server and ViewPoint are concurrently accessing the Wave database in excess of the 8 simultaneous database transactions allowed by Microsoft's MSDE database. You can ignore this message if you only receive 100 or so of these events per day. If you're getting this event hundred of times per day, you should upgrade to the full version of Microsoft SQL Server which doesn't have a limit on the number of simultaneous queries. See Chapter 3 of the *Wave Server Installation Guide* for more information.

100 - Informational
Server Started -- Version ##

An informational message indicating when the Wave Server started.

101 - Informational
Server Stopped

An informational message indicating when the Wave Server was shut down. This message indicates an orderly shutdown, not a shutdown caused by a problem.

105 - Error
No Voice Resource Available

This message indicates that Server was unable to provide a voice resource for a requested operation. This error should not be encountered in normal operation and may indicate that you need additional voice resources for your current load.

106 - Informational
Device ## Restarted

This message indicates a trunk or station was restarted to recover from an error condition. The restart may have been initiated automatically by the Wave Server or manually by the system administrator. If this message is seen only infrequently, it can be ignored. If it is seen often, contact your Wave provider.

111 - Error
Unable to start Mail Server. Voicemail notifications via Email will be disabled.

On startup, the Wave Server was unable to start the e-mail notification process. For example, it could not establish a MAPI connection with your mail post office. Mail notification will be disabled until the problem is resolved. Contact your Wave provider.

112 - Informational
Started Mail Server.

An informational message indicating that the Wave Mail Server started successfully when the Server started.

116 - Error
Server cannot record any more voice messages or calls. Disk space is low.

Wave cannot perform call recording on voice messages or calls, because the disk space on the voice files disk is low.

117 - Informational
Server can now record voice messages and calls. Disk space is available.

Call recording can resume, after having been disabled due to low disk space. Sufficient disk space on the voice files computer is now available.

T-1 alarms

The following two T-1 alarms are written to the Windows Event Log:

- **Red Alarm**. Signals that the Robbed Bit T-1 line has lost synchronization with the switch to which it is connected. Wave disables all channels on the affected digital span so that spurious signals are not processed as incoming calls.
- **Red OK**. Signals that synchronization has been restored. All channels on the affected digital span are re-enabled.

All T-1 alarms are written to the Wave Server logs.

128 - Error
Notification via pager failed; Unable to allocate trunk; user ‘<username>’, number ‘##’, access code ##

An attempt to send a pager notification of a new voice message failed. The error message shows the user’s name and the full dial string of the pager number that was dialed unsuccessfully. Alert the user that the pager number might be incorrect or that pause characters should be added to the dial string.

133 - Error
Device ## is not responding, restarting...

Wave was unable to open the device and is automatically restarting it.

137 - Error
Device ## is not responding.

The trunk or station has stopped responding to events. Try restarting it.

138 - Error
Email notification thread is not responding.

E-mail notifications will be disabled until the problem is resolved.

139 - Error
Device ## Disabled.

This station or trunk was disabled by a user through the Global Administrator.

140 - Informational
Device ## Enabled.

This station or trunk was re-enabled by a user through the Global Administrator.

148 - Error
Removing Failed Sink: <name>

149 - Warning
Database size is nearing critical limit. Archive call log or upgrade to full version of SQL Server.

Your Wave database is nearing the 2GB limit of MSDE. Archive the Call Log to make more room (see “Archiving the Call Log” on page 22-11), or upgrade to the full version of SQL Server if you have not done so already. See the database server requirements in the *Wave Server Installation Guide*

150 - Error
Database size has passed the critical limit and call logging has been stopped. Archive call log or upgrade to full version of SQL Server.

New calls are not being written to the Call Log because the Wave database has passed the critical MSDE size limit (about 2 GB). Archive the Call Log to make more room (see “Archiving the Call Log” on page 22-11), or upgrade to the full version of SQL Server if you have not done so already. See the database server requirements in the *Wave Server Installation Guide*.

155 - Error
Infinite Loop:

Wave detected a Contact Center which may be sending callers back and forth to an extension in an infinite loop. This can happen if the queue redirects callers to an extension whose routing list automatically sends calls to the queue.

157 - Error
Failed to resolve the following email addresses:

An email notification was sent where at least one of the email addresses could not be resolved from a name to an address, for example, an address of “John Smith” could not be resolved as an e-mail address. Possible causes include a mistyped name (for example, “Jhon Smith”), an ambiguous name (for example, “John S”), or a problem with the address book associated with the default MAPI profile on the Wave Server.

158 - Error
Failed to send email. subject:

Wave failed to send the specified email notification. This can happen for numerous reasons, such as a network failure. The specific error is included if available.

164 - Warning
Server cannot communicate with Workstation applications because you have Internet Connection Firewall (ICF) enabled.

For the Wave Server to operate properly with a firewall, you must upgrade your PC to Windows XP SP2 or higher. Alternatively you can disable ICF.

165 - Warning
Server cannot communicate with Workstation applications because Windows Firewall exceptions are not allowed.

Please enable Windows Firewall exceptions by selecting Start > Control Panel >Windows Firewall and deselect the Don't allow exceptions checkbox.

166 - Warning
ISM cannot communicate with Workstation applications due to a problem creating a Windows Firewall exception.

Please disable the Windows Firewall by selecting Start > Control Panel > Windows Firewall and uncheck “On”.

167 - Warning
Server cannot communicate with Workstation applications due to a problem with system DCOM settings.

168 - Warning
Cannot communicate with your <name> Server because you have Internet Connection Firewall (ICF) enabled.

To use this application with a firewall, you must upgrade your PC to Windows XP SP2 or higher. Alternatively you can disable ICF.

169 - Warning
Cannot communicate with your <name> Server because Windows Firewall exceptions are not enabled.

170 - Warning
Cannot communicate with your <name> Server due to a problem creating a Windows Firewall exception.

To use this application please disable the Windows Firewall by selecting Start > Control Panel > Windows Firewall and deselect On.

171 - Warning
Cannot communicate with your <name> Server due to a problem with system DCOM settings.

172 - Warning
Windows networking settings have been updated so the <named> workstation applications can operate properly. You must restart your computer before the new settings will take effect.

176 - Error
Wave is unable process email because it cannot connect to the database.

Wave could not connect to the database after 10 attempts. Possible reason is that email notification may not be working properly.

190 - Warning
The custom N network capture filter is invalid and the default capture filter will be used instead. Ensure that the custom N capture filter was entered properly or contact your N Provider to obtain a valid capture filter.

For more information, see the capture filter syntax in the documentation section of http://www.winpcap.org.

192 - Error
MP3 Conversion Error: <name> in function N.

198 - Warning
Server cannot capture network traffic due to low disk space.

Please make sure N MB of disk space is free for network traffic to be captured.

199 - Informational
Server is now capturing network traffic. Disk space is available.

201 - Error
New voicemail call notification failed for user <name>; Unable to reach <name>.

202 - Warning
Network capture was unable to start because it was unable to discover a valid NIC.

203 - Warning
Network capture was unable to start because no valid WinPCap library.

206 - Error
Server logging has been disabled due to a disk operation error. Failed to open log file ##.

Please check the drive for errors.

207 - Warning
A hard drive partitioned as FAT32 has been detected on the Server.

Please convert the drive to NTFS to ensure mission critical reliability for the Wave Server.

7000 - Error
The dlgcmpd service failed to start due to the following error: The system cannot find the device specified.

7001 - Error
The dlgcmcd service depends on the dlgcmpd service which failed to start because of the following error: The system cannot find the device specified.

Archiving call recordings and voicemail

If you record all calls or even a significant portion of calls, or if you have users with thousands of saved voice messages and large maximum mailbox sizes, disk space on the Wave Server can quickly fill up with voice messages and call recordings. In addition, ViewPoint performance will suffer when managing thousands of recordings, or when recordings are being delivered to the user in quick succession.

To handle thousands or even millions of recordings effectively, Wave lets you archive mailbox recordings (voicemail and call recordings) to a network directory of your choice, called the archive folder. Archiving moves the mailbox recording as well as all information about the recording from the Wave Server to the archive folder, so archived voice messages and call recordings are no longer displayed in ViewPoint. If you are archiving queue mailbox recordings, each queue's recordings are archived to a separate subfolder.

Users can then search for and manage archived recordings using the Wave Archived Recording Browser without burdening the Wave Server, Wave database, or ViewPoint.

You can restore archived recordings to the mailbox of origin or export them to another location. (When an archived recording is restored or exported, it remains in the archive folder until purged.) For more about managing and listening to archived recordings using the Wave Archived Recordings Browser, see Appendix A in the *Wave ViewPoint User Guide*.

This section describes the following:

- Configuring the Wave Recording Archive Service. See page 22-26.
- Starting and stopping the Wave Recording Archive Service. See page 22-30.
- Archiving mailbox recordings. See page 22-31.
- Configuring users who can manage archived recordings. See page 22-35.

See the following related topics in other Wave manuals:

- Installing the Recording Archive Service. See Chapter 10 in the *Wave Server Installation Guide*.
- Using the Archived Recording Browser to search for and act on mailbox recordings. See Appendix A in the *Wave ViewPoint User Guide*.

About the Wave Recording Archive Service

The Wave Recording Archive Service, which manages the archive process, runs on the archive server, a separate PC from the Wave Server. By off-loading archive processing, the Recording Archive Service can handle the resource-intensive archiving process without impacting Wave performance, and can also archive mailbox recordings from multiple Wave Servers.

About mailbox recording file formats

You can archive mailbox recordings in any of the following formats. You can specify which format to use on a user-by-user basis (see “Archiving mailbox recordings” on page 22-31.)

- WAV format is commonly used by Windows applications such as Windows Media Player. (WAV size = 64 Kbps, 469 Kb/minute.)
- MP3 is a popular format that consumes less disk space because of its very high compression rate. The format’s compression ratio makes the MP3 format consume a significant amount of CPU and time when converting files to MP3. (MP3 size = 20 Kbps, 146 Kb/minute.)

Note: Archiving a mailbox recording in MP3 format results in the smallest file size, about one-third the size of archiving the same recording in WAV format.

Searching for and acting on archived recordings

You use the Wave Archived Recording Browser to search and manage archived recordings. To use the Archived Recording Browser, you log on using an archive browser user name and password. For more about archive browser user accounts, see “Configuring users who can manage archived recordings” on page 22-35.

For details on how to use the Archived Recording Browser to search for and act on mailbox recordings (or to import a recording archive from Wave ISM 1.0), see Appendix A in the *Wave ViewPoint User Guide*.

Configuring the Wave Recording Archive Service

Important! Before you can configure the Recording Archive Service, install it as described Chapter 10, “Installing the Wave Recording Archive Service” in the *Wave Server Installation Guide*. Be sure to review the “Requirements” section in that chapter, which details requirements for the archive server PC and archive folder.

To configure the Wave Recording Archive Service

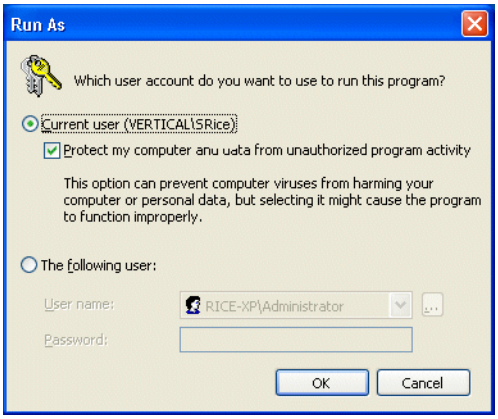
1 On the archive server, choose **Start > Programs > Vertical Wave > Wave Recording Archive Service Manager**.

The Wave Recording Archive Service Manager requires administrative rights to run.

- **If the current user has administrative rights**, a Windows User Account Control (UAC) dialog opens asking the user to confirm that the application should be launched.

  Click **OK** to continue.

- **If the user does not have administrative rights**, a Windows UAC dialog opens asking the user to enter the username and password of a user with administrative rights.



Run As

Which user account do you want to use to run this program?

● Current user (VERTICAL\SRice)

☑ Protect my computer anu uata from unauthorized program activity

This option can prevent computer viruses from harming your computer or personal data, but selecting it might cause the program to function improperly.

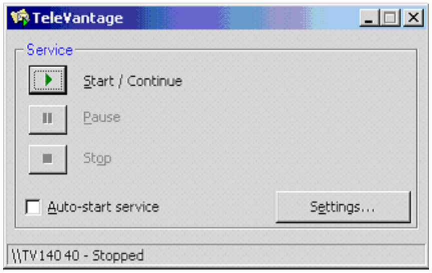
○ The following user:

User name: RICE-XP\Administrator

Password:

Enter that information and click **OK** to continue.

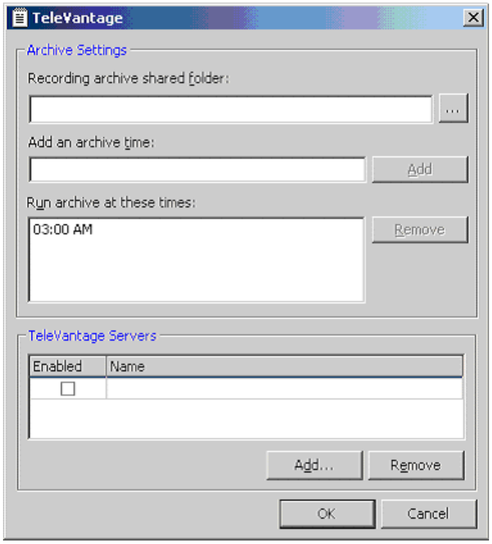
2 The Wave Recording Archive Manager opens:



□ Auto-start service

\\TV14040 - Stopped

3 Click **Settings**. The Wave Recording Archive Service Manager Settings dialog opens:



Recording archive shared folder:

Add an archive time:

Run archive at these times:

03:00 AM

Enabled	Name
□	

4. To specify the **Recording archive shared folder**, Click ... and browse to the archive folder you created (according to the instructions in Chapter 9 in the *Wave Server Installation Guide*). The archive folder is a network folder where mailbox recordings are archived, that must be shared with full read/write permissions to any user who wants to access the recordings. If you are archiving mailbox recordings from multiple Wave Servers, each one archives to an individual subfolder within the archive folder.

5. Specify the time when mailbox recordings will be archived automatically. (The default archive time is 3:00 AM.) You can specify additional archive times if you need to archive more frequently.

   Under **Add an archive time**, enter the time using the format `hh:mm AM` or `PM` and then click **Add** to add it to the **Run archive at these times** list.

   To remove an archive time from the list, select it, and then click **Remove**.

6. To add a Wave Server to the list of Servers from which mailbox recordings will be archived, click **Add**, and then browse to the Wave Server that you want to add.

   When you specify multiple Wave Servers for archiving, archiving occurs on one Wave Server at a time, in the order that the Wave Servers are specified here. Once archiving completes on one Wave Server, it starts on the next Wave Server in the list. Mailbox recordings from all of the Wave Servers are archived to the same archive folder.

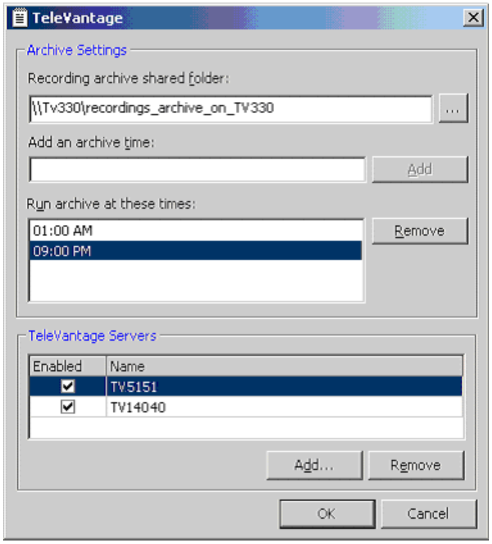
   Note: Each Wave Server name that you specify here is used to populate the **Archiving server** field on that Server's Recording \ Archive tab (**Tools > System Settings** in the User/Group Management applet.) For details, see Section "Message 'Wave Recording Archive Service has not been configured to archive this server' when starting the Global Administrator on the Wave Server" in Appendix B in the *Wave Server Installation Guide*.

   To permanently remove a Wave Server from the list, select it and then click **Remove**. Once removed from the list, you cannot automatically or manually archive mailbox recordings from that Wave Server. To temporarily prevent mailbox recordings on a specific Wave Server from being archived, see the next step.

7 Select the **Enabled** checkbox for each Wave Server that you want to archive automatically.

Note: If **Enabled** is not checked, mailbox recordings will not be archived automatically on the Wave Server, but you can still perform manual archives according to the instructions in "Archiving mailbox recordings manually" on page 22-34.

8 Click **OK** to save your changes.



Recording archive shared folder: \\Tv330\recordings_archive_on_TV330

Add an archive time:

Run archive at these times:
01:00 AM
09:00 PM

Enabled	Name
☑	TV5151
☑	TV14040

Starting and stopping the Wave Recording Archive Service

Caution! *The Recording Archive Service must be running on the archive server in order for an automatic or manual archive to occur. It is recommended that you set the Recording Archive Service to auto-start according to the following instructions.*

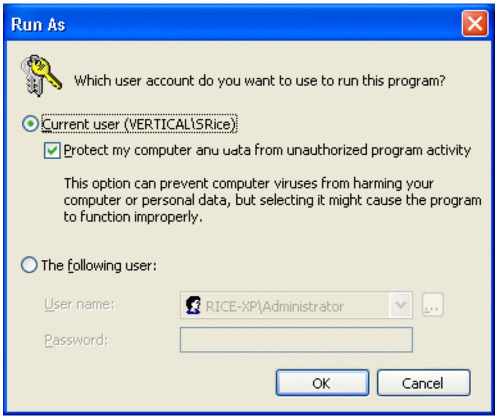
1 On the archive server, choose **Start > Programs > Vertical Wave > Wave Recording Archive Service Manager**.

The Wave Recording Archive Service Manager requires administrative rights to run.

- **If the current user has administrative rights**, a Windows User Account Control (UAC) dialog opens asking the user to confirm that the application should be launched.

  Click **OK** to continue.

- **If the user does not have administrative rights**, a Windows UAC dialog opens asking the user to enter the username and password of a user with administrative rights.



Run As

Which user account do you want to use to run this program?

● Current user (VERTICAL\SRice)

☑ Protect my computer anu uata from unauthorized program activity

This option can prevent computer viruses from harming your computer or personal data, but selecting it might cause the program to function improperly.

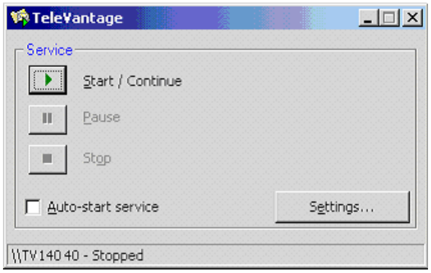
○ The following user:

User name: RICE-XP\Administrator

Password:

Enter that information and click **OK** to continue.

2 The Wave Recording Archive Service Manager opens:



□ Auto-start service

\\TV14040 - Stopped

3 Use the buttons to **Start/Continue**, **Pause**, or **Stop** the Recording Archive Service manually.

Note: If you pause the Archive Recording Service, scheduled or manual archives will not start until you click **Start/Continue** and the Service is running again. If you click **Pause** while a scheduled or manual archive is in process, the Service will show a status of **Pause Pending** until the archive has completed. The status of the Service will then automatically be set to **Paused**.

4 Select the **Auto-start service** checkbox to start the Recording Archive Service automatically whenever the Wave Server starts.

Archiving mailbox recordings

You can archive mailbox recordings automatically according to the settings in the Recording Archive Service Manager, or archive manually at any time. You can modify the mailbox archive settings for an individual user when you set up the archiving event.

Archiving mailbox recordings automatically

Use the User/Group Management applet to configure automatic archiving for various mailboxes according to the following steps.

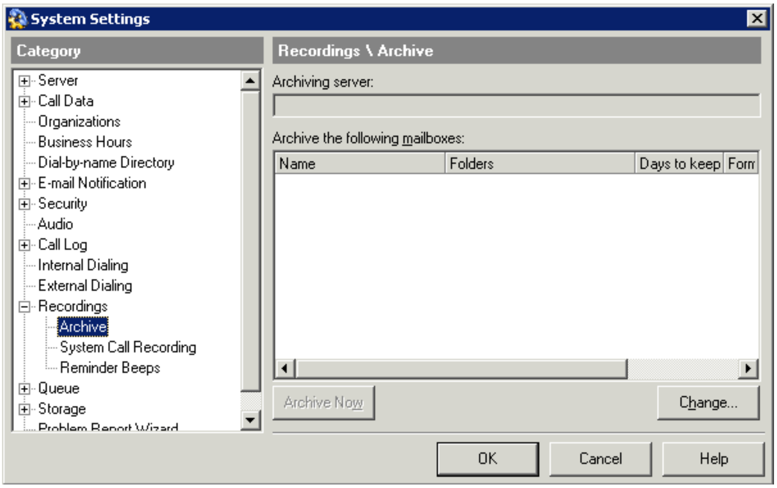
To archive mailbox recordings automatically

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. When the System Settings dialog opens, choose the Recordings \ Archive tab.

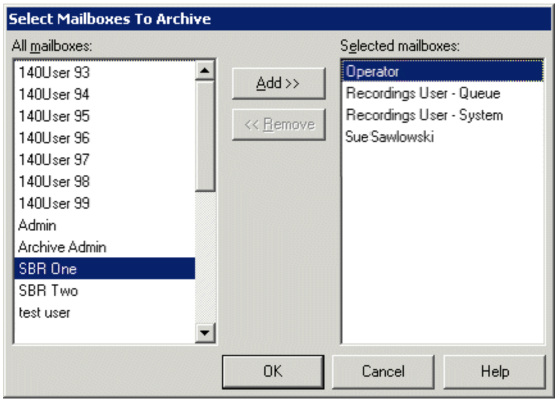


The **Archiving server** field is blank until you configure the Recording Archive Service to include the list of Servers from which mailbox recordings will be archived, according to the instructions in “Configuring the Wave Recording Archive Service” on page 22-26.

If you have configured the Wave Recording Archive Service and the field is still blank, try exiting User/Group Management and logging back on to refresh the field. The configured Archive Server should now appear.

Note: If you set up automatic archiving according to the following steps, archiving will not occur if **Archiving server** is blank, and a message will be displayed to that effect each time you start the User/Group Management applet.

4 The **Archive the following mailboxes** list shows the voice mailboxes that will be automatically archived. To add to or change the list, click **Change**. The Select Mailboxes To Archive dialog opens.



Select Mailboxes To Archive

All mailboxes:

140User 93
140User 94
140User 95
140User 96
140User 97
140User 98
140User 99
Admin
Archive Admin
SBR One
SBR Two
test user

Selected mailboxes:

Operator
Recordings User - Queue
Recordings User - System
Sue Sawlowski

5 Users in the **Selected mailboxes** list will have their mailbox recordings automatically archived. Use the **Add** and **Remove** buttons to modify the list. Click **OK** to return to the Recordings \ Archive tab.

6 To modify the mailbox archive settings for an individual user, click the following column headings for the user in the **Archive the following mailboxes** list:

- **Folders**. Select which of a user’s folders to archive from the drop-down list:
  - **Inbox only.** Only mailbox recordings in the user’s Inbox folder are archived.
  - **All folders except Deleted**. All of the user’s mailbox recordings are archived. (Mailbox recordings in the user’s Deleted folder are never archived.)
- **Days to keep**. Enter the number of days that the user’s recordings remain in the database before being archived. Click the column heading to enter a new number of days.
- **Format**. Click the column heading to select whether to archive the user’s audio files as MP3 or WAV files.

7 Click **OK**.

Archiving mailbox recordings manually

At any time, you can manually archive all mailbox recordings selected for automatic archiving, or a single user’s or queue’s mailbox recordings. (You can archive a single user’s recordings even if the user is not already included in the selected mailbox list used for automatic archiving.)

Use the User/Group Management applet to archive mailbox recordings manually according to the following steps.

To manually archive all selected mailbox recordings

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

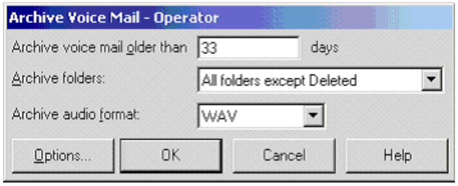
3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the Recordings \ Archive tab.

5 Click **Archive Now**. Wave archives all selected mailbox recordings already specified on the System Settings dialog, Recordings \ Archive tab (see page 22-32).

To manually archive a single user’s or queue’s mailbox recordings

1 In the Users view, select the user and choose **Users > Archive Mailbox Recordings**. For a queue, select it in the Queues view and choose **Queues > Archive Mailbox Recordings**. The Archive Voice Mail dialog opens.



Archive Voice Mail - Operator

Archive voice mail older than 33 days

Archive folders: All folders except Deleted

Archive audio format: WAV

2 Modify any of the following settings:

- **Archive voicemail older than ___ days**. Enter in days which mailbox recordings you want to archive now.
- **Archive folders**. Select which of a user's folders to archive from the drop-down list:
  - **Inbox only**. Only mailbox recordings in the user's Inbox are archived.
  - **All folders except Deleted**. All the user's mailbox recordings are archived, including those in custom folders. Mailbox recordings in the user's Deleted folder are not archived.
- **Archive audio format**. Select whether to archive the user's audio files as MP3 or WAV files.

3 Click **OK** to start archiving the user's mailbox recordings.

Configuring users who can manage archived recordings

Before users can search and act on archived recordings, you must configure one or more archive browser user accounts.

Archive browser user accounts do not necessarily correspond to Wave user accounts, and you do not have to create an archive browser user account for each Wave user who needs to search for and manage archived recordings—multiple Wave users can log on to the Archived Recording Browser simultaneously using the same archive browser user name and password.

Typically, you create several archive browser user accounts, each with different privileges to manage recordings, and then provide the appropriate archive browser user name and password to those Wave users who need to use the Archived Recording Browser. Each account can be shared by multiple Wave users.

Note: You use the Archived Recording Browser to configure user accounts according to the instructions in this section. The first time you run the Archived Recording Browser to configure user accounts, you use a default account with Archive Admin privileges.

To install the Archived Recording Browser

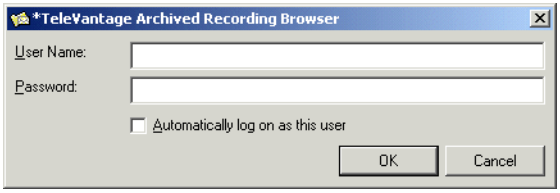
If you have not already done so, install the Archived Recording Browser according to the instructions in Chapter 9 in the *Wave Server Installation Guide*. For administrative purposes, you can install the Archived Recording Browser on the archive server or on another PC.

- The **PC requirements** for the Archived Recording Browser are the same as for ViewPoint, as described in “ViewPoint requirements” in Chapter 9 in the *Wave Server Installation Guide*.
- The **Archived Recording Browser is a Wave workstation application**, installed via the Wave Workstation Applications Setup. In the In the Setup Type dialog, click **Custom** to choose the Archived Recording Browser.

Follow the same instructions to install the Archived Recording Browser on the PCs of users who need to search for and act on archived recordings.

To add new archive browser users

1 Start the Archived Recording Browser by choosing **Start > Programs > Vertical Wave > Wave Archived Recording Browser.** The Wave Archived Recording Browser dialog opens:



*TeleVantage Archived Recording Browser

User Name:

Password:

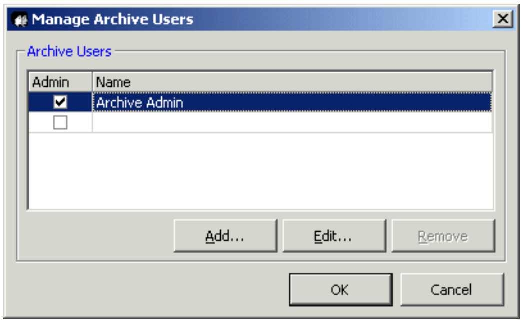
☐ Automatically log on as this user

2 If you are running the Archived Recording Browser for the first time, enter a **User Name** of `Archive Admin`, leave the **Password** field blank, and then click **OK**. Otherwise, log in as any archive browser user with Archive Admin privileges.

Close the Search Archived Recordings dialog when it opens.

Note: If you are running the Archived Recording Browser for the first time, be sure to enter a password for the Archive Admin user for improved security.

3 In the Archived Recording Browser, choose **Tools > Manage Archive Users**. The Manage Archive User dialog opens:



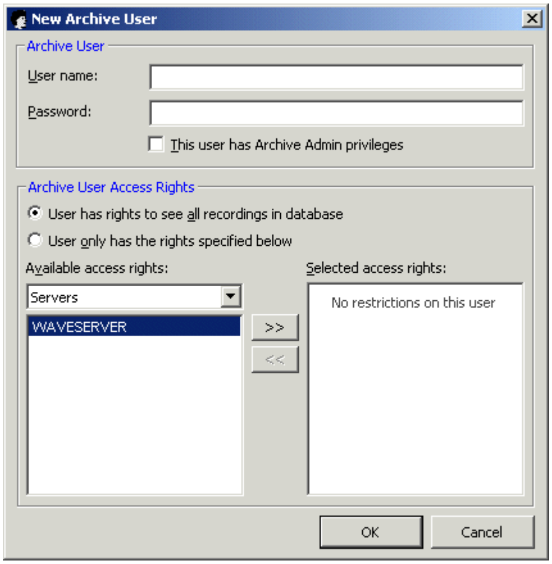
Manage Archive Users

Archive Users

Admin	Name
☑	Archive Admin
□	

4 Password-protect the default Archive Admin user. To do so, select the Archive Admin user, and then click **Edit**. In the Edit Archive User dialog, enter a **Password** and then click **OK** twice to save the new password.

5 To add another archive browser user, in the Archived Recording Browser, choose **Tools > Manage Archive Users**, and then click **Add**. The New Archive User dialog opens:



New Archive User

Archive User

User name:

Password:

□ This user has Archive Admin privileges

Archive User Access Rights

● User has rights to see all recordings in database

○ User only has the rights specified below

Available access rights: Servers

WAVESERVER

Selected access rights:

No restrictions on this user

6. Enter the **User Name** and **Password** for the archive browser user. These do not have to be the user's Wave user name and password (see "Searching for and acting on archived recordings" on page 22-25 for more about archive browser users.)

7. Optionally, check **This user has Archive Admin privileges** if you want the user to be able to add, edit, or delete archive users, or create other Archive Admin users.

8. Click one of the following to specify the user's access rights.

    - **User has rights to see all recordings in database**. Select this option if you want the new user to be able to view and act on all archived mailbox recordings. Click **OK** and then go to step 10.
    - **User only has the rights specified below.** Select this option to limit the new user's access rights to only the options you specify in the next step.

9. Select one of the following from the drop-down list:

    - **Servers**. If given access to a Wave Server, the user can search and manage only the mailbox recordings that were archived from the specified Wave Server.
    - **Archived Mailboxes**. If given access to an Archived Mailbox, the user can search and manage only the mailbox recordings that were archived from the specified Mailbox.
    - **Users and Contacts**. If given access to a user or contact, the user can search and manage all archived voice messages and call recordings involving the specified user or contact.

    To give the user an access right, select it in the **Available access rights** list, and then click >> to add it to the **Selected access rights** list. Repeat this step to give the user all of the access rights required. To remove an access right, select it in the **Selected access rights** list and then click <<.

10. When you are done setting the user's access rights, click **OK**.

11. Add any additional archive browser users by repeating steps 5-10.

Using the Wave Archive Recording Browser

In order to use the Archive Recording Browser to search for and act on archived recordings, you must provide each user with the following information:

- Network location of the archive and have network access to that location.
- User name and password of one or more Archive Recording Browser user accounts.

For instructions on how to use the Archive Recording Browser, see Appendix A of the *Wave ViewPoint User Guide*.

Monitoring database and disk usage

The Wave database stores your system configuration settings (information about trunks, users, auto attendants, and so forth), the Call Log, and an index to voice prompts, greetings, voice titles, and voice message files. The actual voice files themselves are stored separately on disk.

Tasks associated with monitoring database and disk space include:

- Allocating database space
- Allocating disk space

See the *Wave Server Installation Guide* for information on the limits of MSDE and SQL Server databases.

Database server memory usage

The Wave database is configured by default to use up to 50% of the available system memory, which Wave automatically allocates to itself at system startup. Memory size is set when the Wave Server starts. If you add more memory to the system (for example, to support more extensions or trunks), memory size is reset the next time you start the Wave Server.

Memory usage by the database server is dynamic. Some types of database activity (for example, nightly Call Log archiving on busy systems) may require more memory. If more memory is required to support database operations, the database server requests it from Windows. However, this memory is not released automatically when it is no longer needed. For this reason, memory usage by the Wave database typically ramps up to the maximum available, and then levels off. This is normal behavior—not a memory leak—and is not an indication that memory used by the database server is about to reach the maximum or that the system may fail.

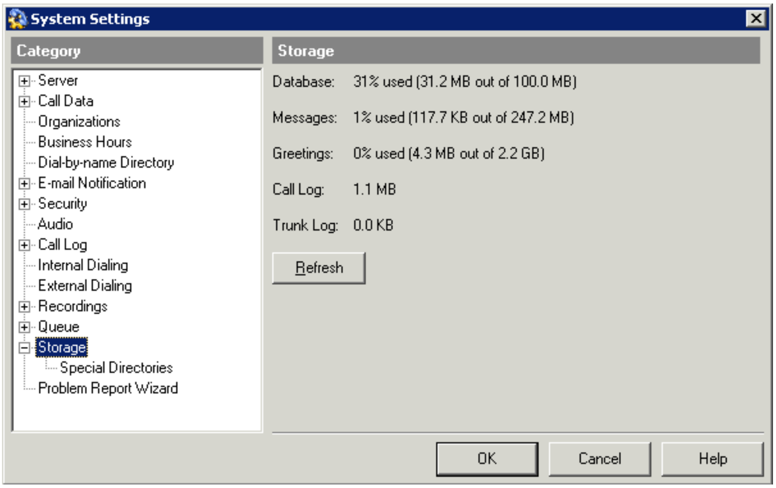
If Windows needs the memory back at a later time for its own use or for another application, it will ask the database server to release some. Also, when you stop the Wave Server, all the memory allocated for use by the database server is released.

Viewing storage statistics

To view how much of the available space your system is currently consuming, do the following:

Click

1. If necessary, click the Administration tab of the Management Console.
2. Click the User/Group Management icon, located in the PBX Administration section of the Management Console.
3. Choose **Tools > System Settings**. The System Settings dialog opens.
4. Choose the Storage tab.



Database: 31% used (31.2 MB out of 100.0 MB)

Messages: 1% used (117.7 KB out of 247.2 MB)

Greetings: 0% used (4.3 MB out of 2.2 GB)

Call Log: 1.1 MB

Trunk Log: 0.0 KB

The tab displays the following information:

- **Database**. Percentage of disk space allocated for the Wave database that is currently used, also shown in kilobytes used out of the total number of kilobytes allocated. The size of the Wave database is set and the required disk space allocated when the Wave Server is installed. The default database size is 100 MB. It will grow automatically up to a maximum of 2 GB if you are using the MSDE database, or to the size of your hard drive if you are using SQL Server Standard or Enterprise editions. See the *Wave Server Installation Guide* for supported databases and requirements.

Note: When you start the User/Group Management applet, Wave displays a warning message if the Wave database is 80% or more full. You should check the database usage periodically to make sure that you are not running out of space. You will also automatically receive e-mail notifications of low space if you have set up Windows Event Log notifications (see “Setting up Wave Event Log notifications” on page 22-16).

- **Messages**. Percentage of disk space currently used for all users’ voicemail messages as well as any call recordings users have made, out of the total amount of space allocated.
- **Greetings**. Percentage of disk space currently used for all users’ greetings and voice titles, out of the total amount of space allocated.
- **Call Log**. Amount of space currently used in the Wave database for Call Log records. Some or all of this space can be recovered by archiving Call Log information if total database usage is high (see “Archiving the Call Log” on page 22-11).
- **Trunk Log**. *This feature is not supported in this version.*

5 Click **Refresh** to refresh the information displayed on the tab.

Changing special Wave directories

You can change the location where Wave stores the following important components on disk:

- Wave Database
- Database transaction log
- Database backup
- Voice files

Note: You must shut down the Wave Server before changing the location of special directories.

To change special Wave directories

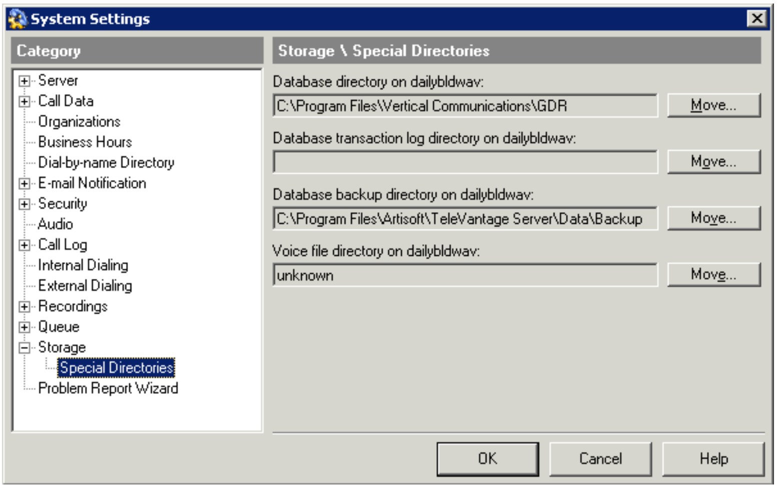
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose The Storage \ Special Directories tab.



Database directory on dailybldwav: C:\Program Files\Vertical Communications\GDR

Database transaction log directory on dailybldwav:

Database backup directory on dailybldwav: C:\Program Files\Artisoft\TeleVantage Server\Data\Backup

Voice file directory on dailybldwav: unknown

5 Click **Move** next to a component to specify a new location for that component.

6 When you are done changing special directory locations, click **OK**.

Identifying password security risks

You can analyze the passwords in use on your system for potential security risks. If you have implemented the security options described in “Securing your system against toll fraud” on page A-3, few users should appear in the list.

For more about system security, see Appendix A, “Protecting Your Phone System Against Toll Fraud.”

To analyze password security risks

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > Analyze Security.**

The Security Analysis dialog lists any users whose passwords may may your system vulnerable, for example a password containing the associated account's extension, a blank password, and so forth.

In addition, each user's logon permissions are displayed (**Logon via trunk**, **Logon via station**, and so forth). Use the scroll bar at the bottom of the dialog to view these columns.

- To change a user's password or other security settings immediately, select the user and then click **Edit** to open the User dialog.
- Click **Copy to Clipboard** to print or save the contents of the dialog.

Reporting problems to your Wave provider

When reporting problems, you may need to supply a variety of Wave log files and other information to facilitate the troubleshooting process. The following sections describe how to assemble and submit this information to your Wave provider.

- **Using the Problem Report Wizard to report a ViewPoint problem**. See page 22-43.
- **Gathering logs to report a Wave problem**. See 22-51.
- **Capturing network troubleshooting logs**. These logs can be useful when troubleshooting client/server or voice-over-IP communications issues. See page 22-55.

Using the Problem Report Wizard

You use the Problem Report Wizard to report any ViewPoint problems to your Wave provider.

Important! The Problem Report Wizard is used for ViewPoint-related problems only. To collect logs for troubleshooting other Wave or Wave Server problems, see "Gathering logs to report a Wave problem" on page 22-51.

The Problem Report Wizard asks you to describe the frequency, patterns, and circumstances of the problem you are reporting. Based on the information you supply, the Problem Report Wizard isolates exactly when and where the problem occurred and automatically collects the appropriate Wave log files and other information from your computer. By assembling all the relevant information, the Wizard helps your provider quickly identify the problem and begin to solve it.

Helping end users to report ViewPoint problems when they occur

Instruct end users to run the Problem Report Wizard in the following ways when they experience a ViewPoint problem:

- **For an issue with a specific call**, right-click on the ViewPoint Call Log entry and choose **Report a Problem**.
- **For a general issue in ViewPoint**, choose **Help > Report a Problem**.
- **If ViewPoint cannot be launched**, choose **Start > All Programs > Vertical Wave ViewPoint > Wave Problem Report Wizard**.

This section discusses the following topics:

- Setting Problem Report Wizard defaults. See page 45.
- Reporting ViewPoint problems. See page 46.
- Reporting problems with specific calls or voice messages. See page 47.
- Flagging a problem call. See page 48.
- The problem report package. See page 49.
- Running the Problem Report Wizard from the command line. See page 50.

Setting Problem Report Wizard defaults

You can set values for the Problem Report Wizard that will be automatically supplied as defaults whenever it is run. The user running the Problem Report Wizard can always override the defaults.

To set Problem Report Wizard defaults

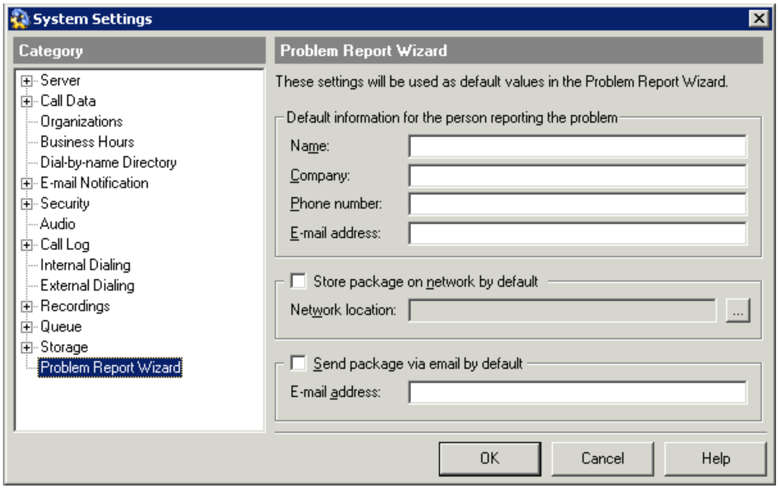
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**. The System Settings dialog opens.

4 Choose the Problem Report Wizard tab.



These settings will be used as default values in the Problem Report Wizard.

Default information for the person reporting the problem

Name:

Company:

Phone number:

E-mail address:

☐ Store package on network by default

Network location: ...

☐ Send package via email by default

E-mail address:

5 Fill in **Default information for the person reporting the problem**.

6 Select one or both of the following checkboxes to specify a default action or actions when a problem report package is created:

- **Store package on network by default**. Specify the default **Network location** where the package will be saved. Click the ... button to browse to a network location.
- **Send package via e-mail by default**. Specify the default **E-mail address** to which the package will be sent.

  Important! Before you can send a problem report package via e-mail, you must first set up e-mail notification via the User/Group Management applet. See “Setting up e-mail notification” on page 4-12.

7 Click **OK**.

Reporting ViewPoint problems

For problems with ViewPoint, run the Problem Report Wizard on the computer that is experiencing the problem.

Examples of ViewPoint problems include:

- ViewPoint behaves unexpectedly.
- User cannot connect to the network.
- User cannot connect to the Wave database.
- ViewPoint does not start.
- ViewPoint closes unexpectedly.
- Data or commands executed in ViewPoint don’t look or behave properly.

Note: For information on how to report a problem with a specific call or voice message, see page 22-47.

To report a ViewPoint problem by running the Problem Report Wizard

1 On the computer that is experiencing the problem, do one of the following to run the Problem Report Wizard:

- From the Start menu, choose **Problems > Vertical Wave ViewPoint > Wave Problem Report Wizard**.
- If you cannot find this shortcut, choose **Start > Run**. Enter the following path and then click **OK**. (The path on your system may be different.)

  ```
  C:\Program Files\Common Files\Vertical\
  Wave\TVPRwizard.exe
  ```
- In ViewPoint, choose **Actions > Report A Problem**.

Note: Running the Problem Report Wizard from ViewPoint only gathers logs from the current ViewPoint session. Running the Problem Report Wizard from the Start menu will pick up the appropriate logs from multiple ViewPoint sessions.

2 Follow the onscreen instructions and answer the questions presented in each Wizard window.

Reporting problems with specific calls or voice messages

Problems with specific calls or voice messages typically involve both ViewPoint running on a user’s computer and the Wave Server. To report these problems, you need to do two things:

- Run the Problem Report Wizard on the user’s computer.
- Collect Wave Server logs as described in “Downloading Wave files” on page 23-22.

Examples of these types of problems include:

- Problems with specific calls in ViewPoint.
- Problems with specific voice messages in a ViewPoint Voice Messages folder.
- Call-handling problems that involve ViewPoint or the Wave Server, for example, calls cannot be conferenced.
- User cannot make outbound calls from ViewPoint.

While you can run the Problem Report Wizard as described on page 22-46 to report any problem, there are several easy ways to report call and voice message problems directly from ViewPoint:

- In the ViewPoint Call Log view, select the problem call (or the call that left the problem voice message), and then choose **Actions > Report a Problem**. The Problem Report Wizard starts with information about the call already entered.
- To report a problem with an active call, select the problem call in the Call Monitor View and then choose **Actions > Report a Problem**. The Problem Report Wizard starts with information about the call already entered.
- If you are very busy, you can alternatively select the problem call in the ViewPoint Call Monitor and click **Flag a Problem** (described below) to automatically gather information about that call, and then run the Problem Report Wizard at a later time.

Flagging a problem call

The **Flag a Problem** button in the ViewPoint Call Monitor lets users click once to flag a problem call, for example, a call that is not displayed correctly in the Call Monitor, or a call in ViewPoint that doesn't match the call on the user's phone.

Flagging a problem call can streamline the problem reporting process, for example if a company operator has too many calls coming in and cannot afford the time away from handling customers to run the Wave Problem Report Wizard for each individual problem call. You can then run the Problem Report Wizard once, at a less busy time, to gather the logs for all of the flagged calls.

To flag a problem call

1. In the ViewPoint Call Monitor, select the problem call.

Click

2. Click the Flag a Problem button on the ViewPoint toolbar. (The Flag a Problem button is located to the left of the Help button at the top of the screen.)
3. If prompted in the Problem Notes dialog, enter notes about the problem, and then click **OK**. (By default, you will not be prompted to enter notes. To configure this behavior, contact your Vertical support representative.)

To gather logs for all flagged calls

1. At a less busy time, run the Wave Problem Report Wizard from the Start menu as described on page 22-46.

   Note: Running the Problem Report Wizard from the Start menu picks up the appropriate logs for any flagged calls across multiple ViewPoint sessions. You can also run the Wizard from within ViewPoint by choosing **Actions > Report a Problem**, but this will only gather the logs for calls flagged during the current ViewPoint session.

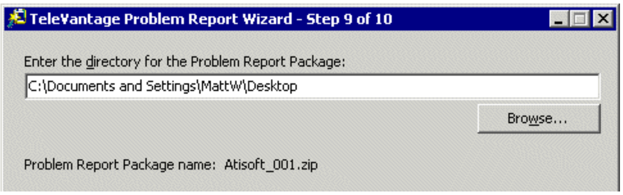
2. Follow the onscreen instructions. On the second Wizard screen, deselect the **This problem involved a specific call or message** checkbox.

The problem report package

The problem report package is a single ZIP file. It contains all the information gathered about the problem by the Problem Report Wizard. The Wizard saves the problem report package to the location you specify.

The Wizard summarizes the information reported, including the date and time the report was created, in a `ProblemInfo.txt` file within the ZIP file. You can open a ZIP file with any zip utility (for example, WinZip).

To prevent problem report packages from being overwritten, the Wizard gives each one a unique name based on your company name and a sequence number.



TeleVantage Problem Report Wizard - Step 9 of 10

Enter the directory for the Problem Report Package:
C:\Documents and Settings\MattW\Desktop

Problem Report Package name: Atisoft_001.zip

E-mailing the problem report package

Optionally, you check **Send Problem Report Package via e-mail** in the final window to e-mail the problem report package to a destination of your choice. Because a problem report package can be large, after you send you should delete it from your system to regain disk space.

Running the Problem Report Wizard from the command line

You can run the Problem Report Wizard without having a Wave application open by running it from the command line. This can be useful for automatically creating scheduled Problem Report Wizard captures using the Windows scheduling service. Run the file `TVPRWizard.exe`, located in `C:\Program Files\Common Files\Vertical\Wave`. You can run the file in the following ways:

- To run the PRWizard normally, specify `\createcab:Yes`. The PRWizard runs with whatever parameters you specify.
- To run the PRWizard automatically, do not include the `\createcab` parameter. The PRWizard runs in the background, with a progress bar showing.

When running the Problem Report Wizard from the command line, you can use any of the following parameters. All are optional.

Parameter	Description
/calllogentry:	Specified Call Log entry from the User/Group Management applet or ViewPoint
/stations:	List of stations involved
/clientpackage:	Full path and filename of a client package to include
/includedatabase:	If Yes, includes a database backup
/estimateddate:	Estimated date of occurrence
/estimatedtime:	Estimated time of occurrence
/exactdate:	Exact date of occurrence
/exacttime:	Exact time of occurrence
/rangestartdate:	Start date of log range
/rangestarttime:	Start time of log range
/rangeenddate:	End date of log range
/rangeendtime:	End time of log range
/summary:	Text summary of the problem
/reproducible:	Whether the problem is reproducible. Enter Yes, No, or Unknown.

Parameter	Description
/details:	Text describing details of the problem
/contactname:	Name of contact at your company
/contactcompany:	Your company
/contactphone:	Your contact phone number
/contactemail:	Your contact email address
/supportname:	Name of your support contact
/supportissue:	Support issue number
/packagepath:	Directory in which to place the ZIP file
/packagefile:	Filename of the ZIP file
/mailpackage:	Whether the package should be e-mailed (not applicable if /createcab is set to Yes)
/createcab:	If Yes then the ZIP file creation will begin automatically
/maxevents:	Maximum number of Event Log events per Event Log type
/cabpriority:	Process priority for cabarc. Enter Normal, Idle, High, Realtime, Below_normal, or Above_normal.

Gathering logs to report a Wave problem

You use the Download applet to download files from the Wave Server to your computer where you can examine them using your Web browser.

These logs are not included in the problem report package created by the Problem Report Wizard (described on page 22-43). You must manually gather them according to the following instructions, and then submit them as directed by your Wave provider.

Depending on your problem, Technical Support may require other logs than the ones describes here. Also, when reporting a ViewPoint problem, be sure to use the Problem Report Wizard, or have the user run it and save the problem report package or e-mail it to you. See “Reporting ViewPoint problems” on page 22-46.

Identifying when a problem occurred

You should narrow the scope of the log file contents down as much as possible to focus on the time period when the problem occurred, because the more extraneous information that you include in a log file, the longer it will take for Tech Support to identify the problem.

Here are two ways to be as specific as possible when identifying *the exact time* when the problem occurred:

- For a time-specific problem (such as a problem with a specific phone call or other error event), ask the user who is experiencing the problem to hang up when the problem occurs, then pick up the phone again and press ** at dial tone.

  Pressing ** does the following:

  - Logs an incident in the Error Log. Examine the Error Log (C:\Program Files\InstantOffice\Logs\error.txt) to identify the exact time that the incident occurred.
  - Starts a new Trace Log. Examine the *previous* Trace Log to verify that the problem was captured.
- If the problem involves a specific call, have the user copy and paste the Call Log entry for the call into an e-mail and send it to you. The information in the Call Log entry will help you gather logs that cover the time period when the problem occurred.

Which logs to gather

Always gather the following logs when reporting a Wave problem—all of these logs can be gathered via the Download applet. The Category and File to download columns indicate the options to select for each log file when you run Download.

Log file name	Category	File to download
IOmanifest.txt	**Log Bundles**	**Current**
Error.log	**Log Bundles**	**Current**
Error.txt	**Log Bundles**	**Current**
Trace.fmt	**Log Bundles**	**Current**
Trace.xxxx.log.Cab	**System Logs**	File covering the date/time range (“xxxx”) during which the problem occurred

Log file name	Category	File to download
TVLOGxxx.txt	**System Logs - Auxiliary**	File covering the date/time range ("xxxx") during which the problem occurred

Important!

- New error.log, error.txt, and trace.fmt files are started each time the Wave Server restarts. If you restarted the Wave Server since the problem occurred, be sure to specify the Log Bundle that covers the time period in question. If you have not restarted the Wave Server, select **Current**.
- Some filenames contain the date/time range covered by the file. For example, Trace.2011-05-19-12-24-27__2011-05-21-04-07-41.log file contains the traces starting on May 19th at 12:24 and continuing to May 21st at 4:07.
- Other filenames contain a sequential number such as TVLog012.txt or TV_Cap_MACADDRESS_007.cap. Look at the date/time stamp in the **Modified** column to determine which file covers the period you are interested in.

Problem-specific log set. Gather the following logs when reporting the indicated specific type of problem:

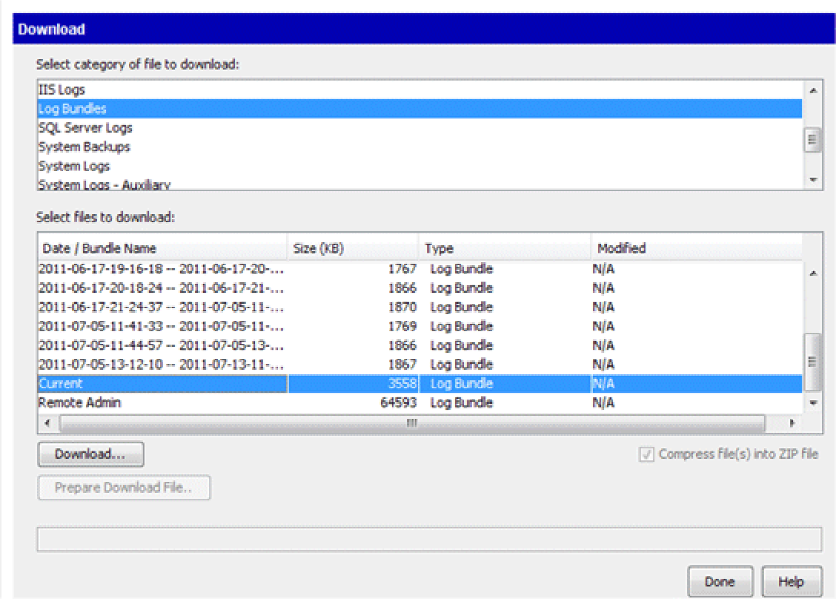
Log file name	Problem type	Category	File to download
TvQueuexxx.txt	Contact Center Queue problem	**System Logs - Auxiliary**	File covering the timeframe during which the problem occurred. Look at the date/time stamp in the **Modified** column to determine which file covers the period you are interested in.
TV_Cap_MACADDRESS_XXXX.cap	VOIP problem	**System Logs - Auxiliary**	
fmlog.xxx.txt	Unexpected Wave Server restart	**System Logs**	
WCAPISVRxxx.log	Viewpoint Mobile App connectivity issues	**System Logs**	
Connectionsxxx.log			
Problem Report Wizard	ViewPoint problems	See "Using the Problem Report Wizard" on page 22-43.	

Other logs. Your technical support representative may request other logs specific to the problem you are experiencing. These can generally be downloaded according to the following instructions as well.

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Download icon, located in the General Administration section.



Download

Select category of file to download:

IIS Logs
Log Bundles
SQL Server Logs
System Backups
System Logs
System Logs - Auxiliary

Select files to download:

Date / Bundle Name	Size (KB)	Type	Modified
2011-06-17-19-16-18 -- 2011-06-17-20-...	1767	Log Bundle	N/A
2011-06-17-20-18-24 -- 2011-06-17-21-...	1866	Log Bundle	N/A
2011-06-17-21-24-37 -- 2011-07-05-11-...	1870	Log Bundle	N/A
2011-07-05-11-41-33 -- 2011-07-05-11-...	1769	Log Bundle	N/A
2011-07-05-11-44-57 -- 2011-07-05-13-...	1866	Log Bundle	N/A
2011-07-05-13-12-10 -- 2011-07-13-11-...	1867	Log Bundle	N/A
Current	3558	Log Bundle	N/A
Remote Admin	64593	Log Bundle	N/A

3 Select a category from the list at the top of the screen.

4 Select a file or group of files from the file list. (See “Which logs to gather” on page 22-52 for more about how to select different types of log files.)

5 Select the **Compress file(s) into ZIP file** check box to compress the files using WinZIP. (If you select more than one file, this option is selected automatically.)

6 Click **Download**.

7 Save the file to your local hard drive.

8 Click **Done**.

Capturing network troubleshooting logs

By default, Wave continually captures network traffic information and write it to logs that can help simplify the troubleshooting of client/server or voice-over-IP communications issues.

Network capture logs capture the following protocols:

- Session Initiation Protocol (SIP).
- Realtime Transport Protocol (RTP). (RTP logging is turned off by default.)
- Trivial File Transfer Protocol (TFTP)
- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP) (H.225, H.245)
- Microsoft Distributed Component Object Module (DCOM)
- Dynamic Host Configuration Protocol (DHCP)
- Bootstrap Protocol (BootP)
- Domain Naming System (DNS)

When network capture is enabled, a separate series of log files is written for each network interface card (NIC) in the Wave Server PC. By default, each series consists of 20 files of 32 MB each, and the files are continually overwritten starting with the oldest file. The filenames of the captured traces are in the format `Tv_cap_nnnnnnnnnnnn_00xx.cap`, where `nnnnnnnnnnnn` represents the last 12 digits of the WinpCap NIC ID, and `00xx` represents the capture number (for example, 0001, 0002 ...0020). An example of a log file name is:

```
Tv_cap_1E2F3B4A5C85_0010.cap
```

Note: Network capture logs are not included in the problem report package created by the Problem Report Wizard (described on page 22-43). You must manually gather and submit network capture logs as directed by your Wave provider.

Adjusting or turning off network capture

In the User/Group Management applet, you can adjust the number and size of the log files or files or turn off network capture completely.

To adjust or turn off network capture

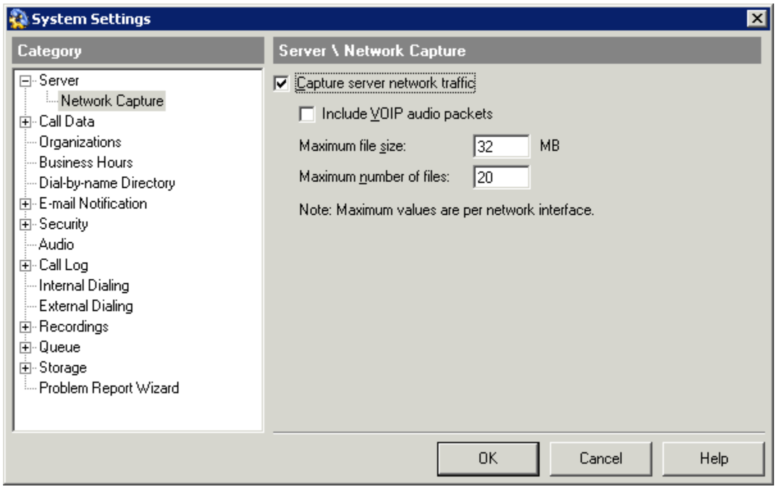
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User/Group Management icon, located in the PBX Administration section of the Management Console.

3 Choose **Tools > System Settings**.

4 Click the Server \ Network Capture tab.



System Settings

Category

Server
- Network Capture

Call Data
Organizations
Business Hours
Dial-by-name Directory
E-mail Notification
Security
Audio
Call Log
Internal Dialing
External Dialing
Recordings
Queue
Storage
Problem Report Wizard

Server \ Network Capture

☑ Capture server network traffic

□ Include VOIP audio packets

Maximum file size: 32 MB

Maximum number of files: 20

Note: Maximum values are per network interface.

5 When the **Capture server network traffic** checkbox is selected, you can modify any of the following settings:

- **Include VOIP audio packets**. Select this checkbox to have the logs capture the audio portion of Voice-over-IP calls (RTP protocol.) This option is turned off by default because it can cause network capture files to fill up quickly. Select this option only if you are experiencing problems with voice quality issues on VoIP calls.

  Note: Only RTP traffic on the Wave Server's VAM is captured. RTP traffic handled by any Media Resource Modules (MRMs) installed on the Wave Server is not captured.

- **Maximum file size**. Specify the maximum size on megabytes of each log file before Wave increments the file number and begins writing to a new log file.
- **Maximum number of files**. Specify the total number of log files to be maintained on the system at any one time. When that number is reached, Wave begins overwriting the existing log files starting with the oldest.

6 To disable network capture, deselect the **Capture server network traffic** checkbox.

7 Click **OK**.

Chapter 23

Continuing System Administration

Chapter Contents

This chapter provides background and step-by-step procedures for performing general administrative tasks and monitoring system performance.

Restoring your system configuration

Use System Backup/Restore to restore Wave to the configuration it had when you last did a backup if a power loss has corrupted the database. The restore operation restores from the last backup cabinet (CAB) file located in `C:\inetpub\ftproot\private\iocabfiles`.

Note: You can only restore a system configuration at the same version as your current system—the version number, Service Pack number, and Hot Fix level must all match.

To restore Wave

1 Manually restore the following items:

- Network adapters and settings (including host name/machine name, setting the TCP/IP domain, and IP Address/Subnet Mask/Gateway per adapter. Adapters include: Integrated Services Card)
- Wave account user names and passwords in the Password Administration applet.
- The system date, time, and time zone in the Date and Time applet.
- RAID-1 Configuration (disk mirroring).
- Windows Workgroup or Network Domain

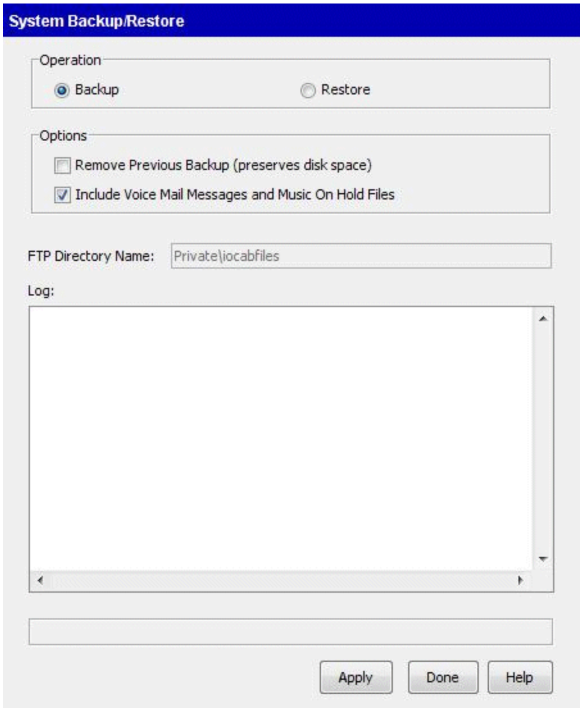
2 If you are restoring from a backup CAB file that was saved in a location external to the Wave Server, make sure that the backup CAB file (Iobackup.cab) is located in the `C:\inetpub\ftproot\private\iocabfiles` directory on your Wave Server.

If this folder does not exist, create it and copy or FTP the CAB file into the directory. Or, just run the backup and the folder will be created automatically.

3 If necessary, click the Administration tab of the Management Console.

Click

4 Click the System Backup/Restore icon, located in the General Administration section of the Management Console.



System Backup/Restore

Operation

● Backup ○ Restore

Options

□ Remove Previous Backup (preserves disk space)

☑ Include Voice Mail Messages and Music On Hold Files

FTP Directory Name: Private\iocabfiles

Log:

5 Select **Restore**.

6 Check **Include Voice Mail Messages and Music on Hold Files** to restore the voicemail messages and Music on Hold WAV files from the backup file.

7 Check **Include Call Navigator Prompts** to restore Call Navigator prompt files from the backup file.

8 Click **Apply**.

9 Click **Yes** to confirm the Restore operation.

Detailed results of the operation will appear in the Log.

10 Click **OK** at the end of the restore process to reboot the Wave Server.

Restoring network settings after using the System Recovery Disk

In the event that you need to use the Vertical Wave System Recovery Disk that came with your system, you will need to restore your customized settings using the System Backup/Restore applet with a previously created backup file. In some cases, you may need to manually reconfigure your network settings and adapter information.

After you have restored your settings using the System Backup/Restore applet (see “Restoring your system configuration” on page 23-2), a log is displayed in the applet that provides information about the Restore action. If Wave could not restore your network adapter information successfully, the log will include the following error message:

```
Error: Cannot Restore Network Adapters
```

If the error message does not appear in the log, then Wave successfully completed the restore operation and you do not need to manually reconfigure your network settings.

To restore your network settings

1 Print or write down the network settings information in the log file.

The information in the log that you will need looks like this, but has values specific to your Wave Server.

```
Hostname=EastCoastIO
Domain=domain.com
NameServer=192.168.1.2 192.168.1.3
SearchList=domain.com
[(Slot 6 + 5) 10/100 Base-T Ethernet Integrated Services Card
  3]
IPAddress=192.168.75.4
DefaultGateway=192.168.75.1
SubnetMask=255.255.255.0
Primary WINS=192.168.1.2
Secondary WINS=192.168.1.3
[[Unknown, DLCI 16] Untitled]
IPAddress=192.168.74.1
```

```
DefaultGateway=
SubnetMask=255.255.255.0
Primary WINS=
Secondary WINS=
```

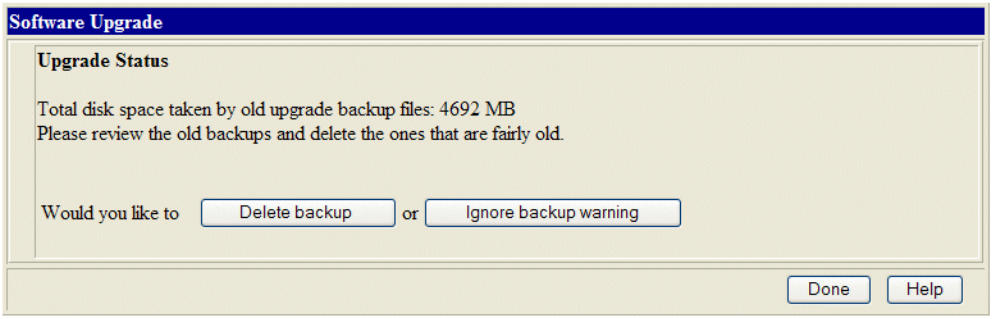
2 Reconfigure your system name and IP addresses for each of your network adapters with the information in the log.

Upgrading or downgrading the Wave Server

You use the Software Upgrade applet to:

- **Upgrade the Wave Server** with a new release of Wave ISM, Service Pack, or HotFix. See “Upgrading the Wave Server” on page 23-6.
- **Downgrade the Wave Server** to rollback to a previous version of Wave ISM. See page 23-22.
- **View a history of all upgrades** that have been performed. See “Viewing upgrade history” on page 23-16.
- **Delete one or more of the system backup files** that are created automatically whenever an upgrade is performed. See “Deleting system backups created during an upgrade” on page 23-17.

When you start the Software Upgrade applet, the Upgrade Status dialog displays the total disk space taken up by old upgrade backup files. (Backup files are created automatically whenever you perform an upgrade.)


Software Upgrade

Upgrade Status

Total disk space taken by old upgrade backup files: 4692 MB
Please review the old backups and delete the ones that are fairly old.

Would you like to

Click **Ignore backup warning** and then click **Done** to continue. Click **Delete Backup** to delete some or all of the old upgrade backup files. See “Deleting system backups created during an upgrade” on page 23-17.

Upgrading the Wave Server

Wave software upgrades are distributed in a cabinet (CAB) file, a compressed archive that includes all of the files required for the upgrade.

Obtaining a CAB file

You can obtain an upgrade CAB file in either of the following ways:

- Via an Upgrade CD that you obtain from your Wave provider.
- By downloading the upgrade CAB file from the Vertical Web site.

For information about a specific upgrade, see the Release Notes included with that base release, HotFix, or Service Pack.

Upgrading the Wave Server consists of the following:

- Uploading the CAB file to the Wave Server. See “Uploading a CAB file” on page 23-7.
- Performing the upgrade. See “Performing an upgrade” on page 23-8.

Scheduling an upgrade

You can choose to perform the upgrade immediately after the upload, or you can upload at one time (for example, during your lunch hour), and then upgrade later when the system is not in use.

- Uploading does not interrupt phone or data services running on the Wave Server.
- The upgrade process includes multiple system restarts, so you should schedule your upgrade so that normal phone service will not be interrupted.

Uploading a CAB file

Before you can perform an upgrade, you must upload the CAB file to the Wave Server and add it to the Upgrade List (the list of upgrades that will be performed).

There are three ways to upload the CAB file:

- **Upload from a file**. When you choose this method, the CAB file you specify is first transferred from the source location to the PC you are using to run the Global Administrator Management Console, and then to the Wave Server. The file to upload can be a local file or a file from another network. This is the slowest upgrade method.
- **Network share**. When you choose this method, the CAB file is transferred directly from the source location to the Wave Server. You need to provide network credentials (user name and password) to access the network location. This method is faster than a client upload, but slower than using a removable drive.
- **Removable drive**. This option is only available if a removable flash drive or CD/DVD drive containing the CAB file has been inserted into the USB port on the Wave Server. When you choose this method, the CAB file on the drive is copied directly to the Wave Server. This is the fastest upgrade method.

  A USB flash drive or CD/DVD drive may contain a “packing list”, a builder-generated list of upgrades contained on the drive. If a packing list is detected on the drive, the CAB files are automatically uploaded to the Upgrade List in the order specified, so you don’t have to add the CAB files to the Upgrade List individually.

How long does an upgrade take?

Upload time is based on file size and the transfer method used.

- Uploading from a removable drive is the fastest method.
- Uploading from a network share is slower than using a removable drive.
- Uploading from a file is the slowest method.

Upgrade time is the same regardless of which method you used to upload.

Note the following:

- Uploading a large CAB file using your browser over the LAN can take an hour or more. Upgrading from a remote source (such as over the Internet) generally takes about three times as long as upgrading from a USB flash drive or CD/DVD that is directly inserted into or attached to the Wave Server.
- When you upload the file using a Web browser, a spinning icon is your only status indicator. Unless your Web browser reports an error, the file upload is probably working fine, so do not interrupt the upload.
- If you are planning to upgrade over a modem connection, be sure to check the size of the upgrade CAB file. Uploads will take the longest over a modem. For example, if the upgrade CAB file is 20 MB, expect a two-hour upload over a modem. For this reason, only small HotFixes should be uploaded using a modem.

For instructions on how to upload a CAB file, see “Uploading and upgrading steps” on page 23-9.

Performing an upgrade

The automated upgrade procedure unpacks files, starts the SNMP Alarms applet (which runs throughout the process so you can monitor the upgrade status), restarts the Wave Server, copies files, restarts again, and verifies the upgrade. In addition, Wave may exercise an option to automatically break and restore the disk mirror with the redundant hard drive for subsequent upgrades, so that if the upgrade fails you can boot with your previous software version from the second drive.

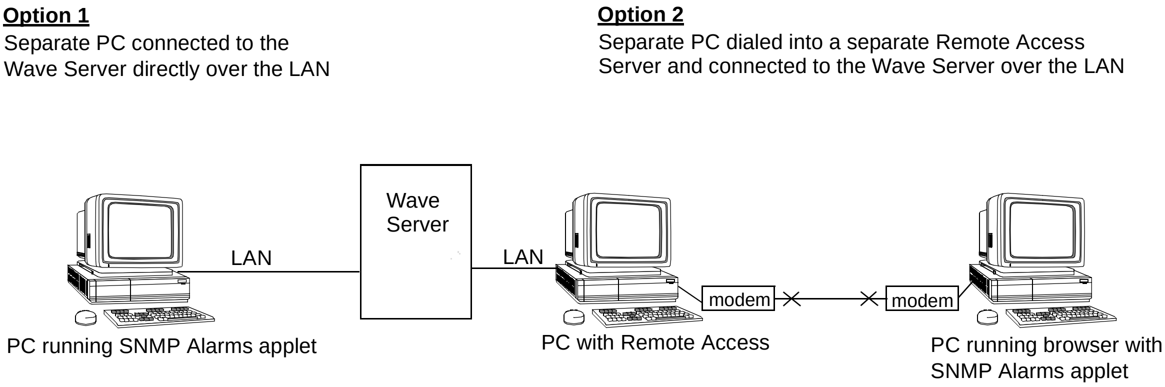
Note: When you start an upgrade, the SNMP Alarm panel pops up and you can monitor the progress of your upgrade. If you have a browser pop-up blocker on your system, the SNMP Alarm panel is blocked and doesn't come up. You can usually configure these blockers to allow pop-ups from specific domains and IP addresses.

The upgrade checks the Wave software versions only. It does not check individual file versions. The registry, Call Detail Report database, and files are backed up as they are replaced. If the upgrade is successful and Wave is fully functional, the setup files are removed.

If you have mirrored disks, use the Disk Management to verify the health of your disks before proceeding with an upgrade. For information about checking your disks using Disk Management, refer to “Identifying RAID disk health” on page 23-40.

Caution! *You cannot see any SNMP alarms during an upgrade unless trap destinations are configured in the SNMP Configuration applet. For instructions, see “Configuring SNMP agents” on page 23-27. In addition, be sure to run the Software Upgrade applet over the LAN or modem, as shown in the next diagram, if you want to view SNMP status.*

The following diagram shows the options for viewing SNMP status:


Option 1
Separate PC connected to the Wave Server directly over the LAN
Option 2
Separate PC dialed into a separate Remote Access Server and connected to the Wave Server over the LAN
Wave Server
LAN
LAN
modem
modem
PC running SNMP Alarms applet
PC with Remote Access
PC running browser with SNMP Alarms applet

For instructions on how to perform an upgrade, see “Uploading and upgrading steps” on page 23-9.

Uploading and upgrading steps

This section describes how to do the following:

- Upgrading from a removable drive. See page 23-10.
- Upgrading from a network share. See page 23-12.
- Upgrading from a file. See page 23-14.
- Upgrading the Wave Server at a later time. See page 23-15.

Upgrading from a removable drive

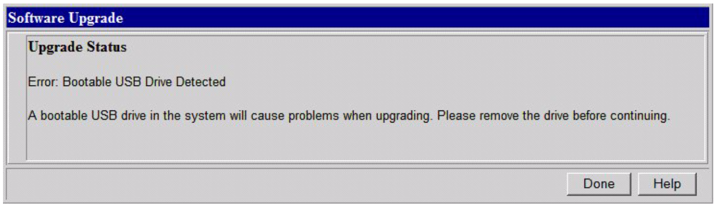
This option transfers the CAB file or files on the USB device directly to the Wave Server. After uploading, you can perform the upgrade immediately, or at a later time. For more about upload and upgrade options, see "Upgrading the Wave Server" on page 23-6.

To upgrade from a removable drive

1 Obtain a flash drive or CD/DVD with the latest version of the upgrade CAB file from your Wave provider.

2 Insert the flash drive or CD/DVD drive into the USB port on the Wave Server.

Note: If you connect a bootable drive via the USB port,



Software Upgrade

Upgrade Status

Error: Bootable USB Drive Detected

A bootable USB drive in the system will cause problems when upgrading. Please remove the drive before continuing.

3 Log on to the Global Administrator Management Console.

Note: To upgrade Wave ISM software, you must have the Wave permission to run the Software Upgrade applet.

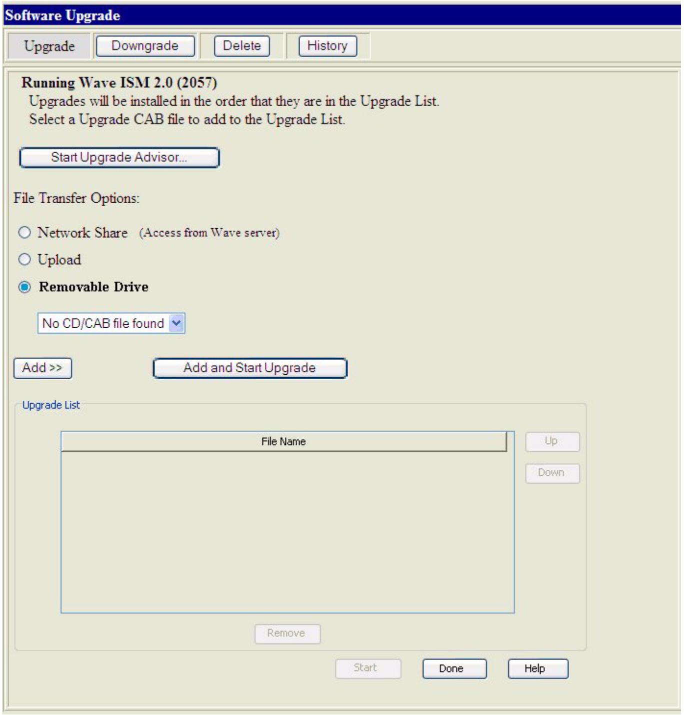
4 If necessary, click the Administration tab of the Management Console.

Click

5 Click the Software Upgrade icon, located in the General Administration section.

6 Select the **Upgrade** button if necessary.

7 In the File Transfer Options section, click **Removable Drive**. This option is only available if a removable device is inserted in the USB port on the Wave Server.



Running Wave ISM 2.0 (2057)
Upgrades will be installed in the order that they are in the Upgrade List.
Select a Upgrade CAB file to add to the Upgrade List.

File Transfer Options:
○ Network Share (Access from Wave server)
○ Upload
● **Removable Drive**

No CD/CAB file found

8 Do one of the following:

- Click **Add>>** to add the CAB files on the USB device to the Upgrade List. To run the upgrade later, see “Upgrading the Wave Server at a later time” on page 23-15.
- Click **Add and Start Upgrade** to add the CAB files on the USB device to the Upgrade List and start the upgrade immediately.

9 After the upgrade is complete, close all browser windows, and then run the Global Administrator Management Console again to review the upgrade history (see “Viewing upgrade history” on page 23-16.) You can also optionally delete backup files are created automatically whenever you perform an upgrade (see “Deleting system backups created during an upgrade” on page 23-17).

Upgrading from a network share

This option transfers the CAB file or files that you specify directly from the network location to the Wave Server. After uploading, you can perform the upgrade immediately, or at a later time. For more about upload and upgrade options, see “Upgrading the Wave Server” on page 23-6.

To upgrade from a network share

1 Log on to the Global Administrator Management Console.

Note: To upgrade Wave ISM software, your user account must have permissions to run the Software Upgrade applet.

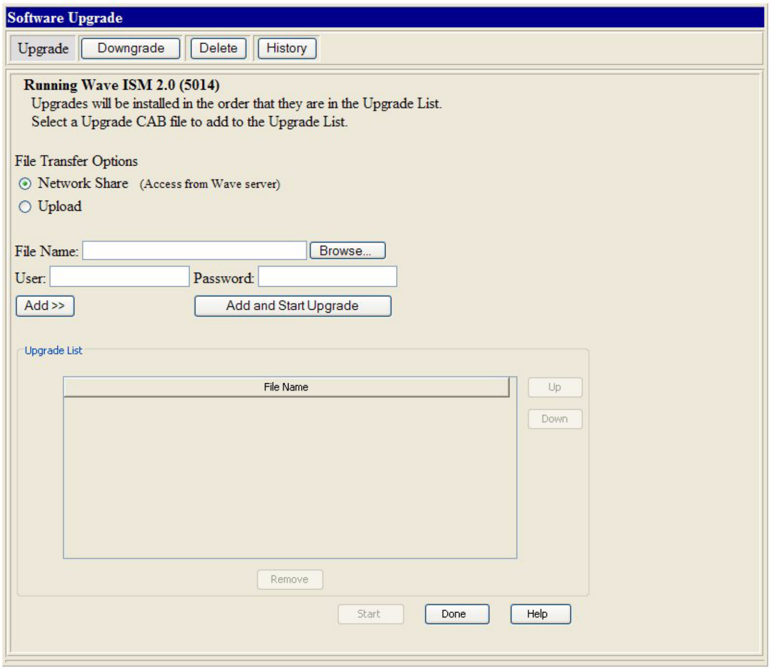
2 If necessary, click the Administration tab of the Management Console.

Click

3 Click the Software Upgrade icon, located in the General Administration section.

4 Select the **Upgrade** button if necessary.

5 In the File Transfer Options section, click **Network Share**.



Software Upgrade

Running Wave ISM 2.0 (5014)

Upgrades will be installed in the order that they are in the Upgrade List.

Select a Upgrade CAB file to add to the Upgrade List.

File Transfer Options

● Network Share (Access from Wave server)

○ Upload

File Name:

User: Password:

6 The **Network Share** option does not work with mapped drives because of network mapping and credential restrictions. You must do one of the following to specify the CAB file:

- Enter the path to the upgrade CAB file in the **File Name** field.
- Click **Browse** to identify it.

If you use the **Browse** button you must do the following:

a Enter the network drive name (for example, \\netdriv1).

b Press **Enter**.

c Click **Browse** and then select path and file of the CAB file to upload.

7 Enter your logon credentials (**User** and **Password**) required to access the network share. If the file is located on the Wave Server itself, no network credential are required.

8 Do one of the following:

- Click **Add>>** to add the CAB file to the Upgrade List. To run the upgrade later, see “Upgrading the Wave Server at a later time” on page 23-15.
- Click **Add and Start Upgrade** to add the CAB files on the USB device to the Upgrade List and start the upgrade immediately.

9 After the upgrade is complete, close all browser windows, and then run the Global Administrator Management Console again to review the upgrade history (see “Viewing upgrade history” on page 23-16.) You can also optionally delete backup files are created automatically whenever you perform an upgrade (see “Deleting system backups created during an upgrade” on page 23-17).

10 After your Wave Server is back online, click **Done** in the Software Upgrade dialog to close the Software Upgrade applet.

Upgrading from a file

This option transfers the CAB file or files you specify from the source location to the PC you are using to run the Global Administrator Management Console, and then to the Wave Server. After uploading, you can perform the upgrade immediately, or at a later time. For more about upload and upgrade options, see “Upgrading the Wave Server” on page 23-6.

To upgrade from a file

1 Log on to the Global Administrator Management Console.

Note: To upgrade Wave ISM software, your user account must have permissions to run the Software Upgrade applet.

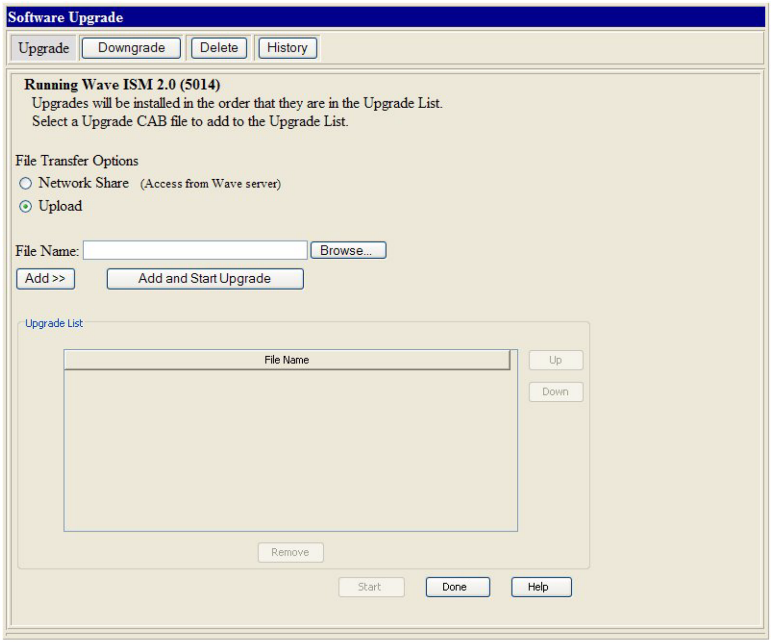
2 If necessary, click the Administration tab of the Management Console.

Click

3 Click the Software Upgrade icon, located in the General Administration section.

4 Select the **Upgrade** button if necessary.

5 In the File Transfer Options section, click **Upload**.



Software Upgrade

Running Wave ISM 2.0 (5014)
Upgrades will be installed in the order that they are in the Upgrade List.
Select a Upgrade CAB file to add to the Upgrade List.

File Transfer Options
○ Network Share (Access from Wave server)
● Upload

File Name:

6. Enter the path to the upgrade CAB file in the **File Name** field, or click **Browse** to identify it.
7. Do one of the following:
   - Click **Add>>** to add the CAB file to the Upgrade List. To run the upgrade later, see “Upgrading the Wave Server at a later time” on page 23-15.
   - Click **Add and Start Upgrade** to add the CAB files on the USB device to the Upgrade List and start the upgrade immediately.
8. After the upgrade is complete, close all browser windows, and then run the Global Administrator Management Console again to review the upgrade history (see “Viewing upgrade history” on page 23-16.) You can also optionally delete backup files are created automatically whenever you perform an upgrade (see “Deleting system backups created during an upgrade” on page 23-17).
9. After your Wave Server is back online, click **Done** in the Software Upgrade dialog to close the Software Upgrade applet.

Upgrading the Wave Server at a later time

Perform the following steps to upgrade the Wave Server using a CAB file that you previously uploaded and added to the Upgrade List.

To upgrade the Wave Server a later time

1. If necessary, click the Administration tab of the Management Console.
2. Click the Software Upgrade icon, located in the General Administration section.

Click

3. Click **Start**. The upgrade begins immediately.
4. After the upgrade is complete, close all browser windows, and then run the Global Administrator Management Console again to review the upgrade history (see “Viewing upgrade history” on page 23-16.) You can also optionally delete backup files are created automatically whenever you perform an upgrade (see “Deleting system backups created during an upgrade” on page 23-17).
5. After your Wave Server is back online, click **Done** in the Software Upgrade dialog to close the Software Upgrade applet.

Viewing upgrade history

The History pane of the Software Upgrade applet displays a history of all upgrades that have been performed. It shows the date and time of current versions as well as when upgrades were started and when they completed successfully.

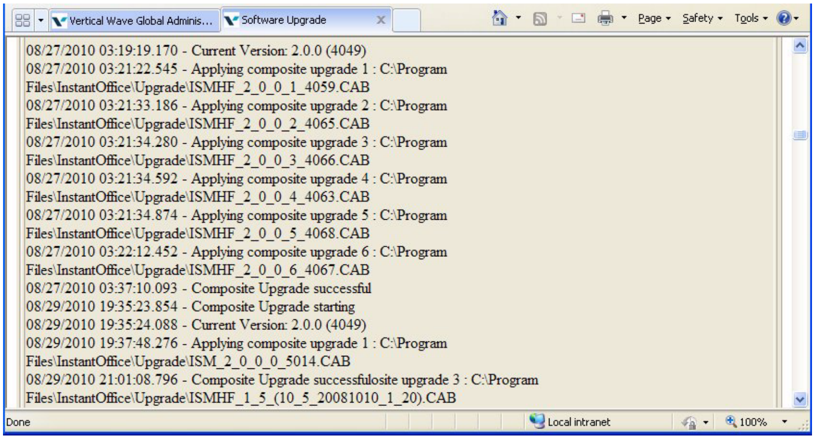
To view upgrade history

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Software Upgrade icon, located in the General Administration section of the Management Console.

3 Click **History.**



```
08/27/2010 03:19:19.170 - Current Version: 2.0.0 (4049)
08/27/2010 03:21:22.545 - Applying composite upgrade 1 : C:\Program
Files\InstantOffice\Upgrade\ISMHF_2_0_0_1_4059.CAB
08/27/2010 03:21:33.186 - Applying composite upgrade 2 : C:\Program
Files\InstantOffice\Upgrade\ISMHF_2_0_0_2_4065.CAB
08/27/2010 03:21:34.280 - Applying composite upgrade 3 : C:\Program
Files\InstantOffice\Upgrade\ISMHF_2_0_0_3_4066.CAB
08/27/2010 03:21:34.592 - Applying composite upgrade 4 : C:\Program
Files\InstantOffice\Upgrade\ISMHF_2_0_0_4_4063.CAB
08/27/2010 03:21:34.874 - Applying composite upgrade 5 : C:\Program
Files\InstantOffice\Upgrade\ISMHF_2_0_0_5_4068.CAB
08/27/2010 03:22:12.452 - Applying composite upgrade 6 : C:\Program
Files\InstantOffice\Upgrade\ISMHF_2_0_0_6_4067.CAB
08/27/2010 03:37:10.093 - Composite Upgrade successful
08/29/2010 19:35:23.854 - Composite Upgrade starting
08/29/2010 19:35:24.088 - Current Version: 2.0.0 (4049)
08/29/2010 19:37:48.276 - Applying composite upgrade 1 : C:\Program
Files\InstantOffice\Upgrade\ISM_2_0_0_0_5014.CAB
08/29/2010 21:01:08.796 - Composite Upgrade successfulosite upgrade 3 : C:\Program
Files\InstantOffice\Upgrade\ISMHF_1_5_(10_5_20081010_1_20).CAB
```

Deleting system backups created during an upgrade

Backup files are created automatically whenever you perform an upgrade. You can delete all of the backup files associated with a specific upgrade to regain disk space.

Important! All backup files older than the one you select to delete will be deleted as well.

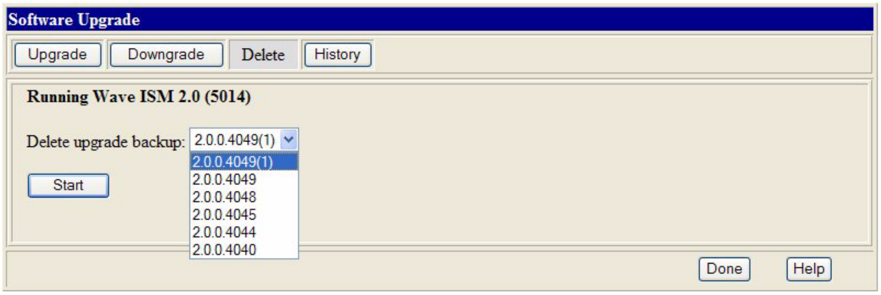
To delete upgrade backup files

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Software Upgrade icon, located in the General Administration section.

3 Click **Delete**.



Software Upgrade

Running Wave ISM 2.0 (5014)

Delete upgrade backup: 2.0.0.4049(1)

4 From the **Delete Upgrade Backup** drop-down list, select the backup that you want to delete.

5 Click **Start**. Repeat these steps to delete backup files from other upgrades.

Downgrading the Wave Server

Downgrading the Wave Server to a previous version of Wave ISM is not recommended. All backups used for a downgrade are removed during the downgrade to prevent you from attempting a subsequent downgrade which could render your Wave system inoperable.

During the downgrade process, the SNMP Alarms applet provides status. As in the upgrade process, the Wave Server is restarted twice while a downgrade is performed.

Caution! *When you downgrade to the software version that was originally shipped with your Wave Server, you also replace your registry with the registry that was shipped with your Wave Server, and you will lose your configuration information.*

To downgrade the Wave ISM software

1 If necessary, click the Administration tab of the Management Console.

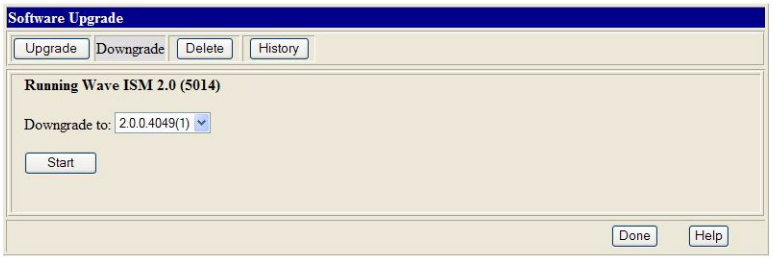
Click

2 Click the Software Upgrade icon, located in the General Administration section.

Note: To downgrade the Wave ISM software, you must log on with an Wave user account that has permission to access the Software Upgrade applet.

The Software Upgrade applet starts.

3 Click **Downgrade**.



Running Wave ISM 2.0 (5014)

Downgrade to: 2.0.0.4049(1)

4 Select the Wave ISM version to downgrade to from the drop-down list. If it is not possible to downgrade, no version will be listed.

5 Click **Start**.

A Downgrade Status message is displayed, and immediately afterwards, the SNMP applet starts so you can monitor the process of the downgrade.

Note: The downgrade procedure reboots the Wave Server twice.

6 After your Wave Server is back online, click **Done** in the Software Upgrade dialog to close the Software Upgrade applet.

Displaying software versions

You will typically access the Software Versions applet when you are troubleshooting an issue, to poll for a list of installed software, or to determine the need to download patches or software upgrades. The Software Versions applet lists the contents of the iomanifest.txt file, which details the product version number, as well as the software (the latest CAB file) installed in Wave.

To check software versions

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Software Versions icon, located in the General Administration section.

3 Scroll through the file until you find the software you want to check.

4 Click **Done** to the Management Console.

Viewing the Fault Monitor Error Logs

The Fault Monitor is an embedded processor that provides independent watchdog services for the overall system, collecting system error messages that help you determine why a fault has occurred. The fault monitor module stores a copy of a subset of the system traces that are stored by the system trace manager, specifically those that are flagged as severe or fatal errors.

The Fault Monitor module must be connected to an analog trunk in order to use dial-in access and pager notification. For information on connecting the Fault Monitor module to a trunk, refer to the *Wave Server Installation Guide*. For a full discussion of using the Fault Monitor, refer to the *Wave Server Hardware Reference Guide*.

The fault monitor module stores copies of a subset of the system traces that are stored by the system trace manager, specifically those that are flagged as severe or fatal errors. The Fault Monitor main buffer is implemented as a circular buffer so that it always contains the most current traces. The buffer is 28 K bytes, and can contain around 250 traces, depending on the size of each trace. On each reboot, the entire contents of this buffer is saved to the file fmlog.*.txt, where the `*` represents the date and time the traces were saved. You can find the fmlog.*.txt files on the Wave Server hard drive in the `C:/Program Files/InstantOffice/Logs` directory.

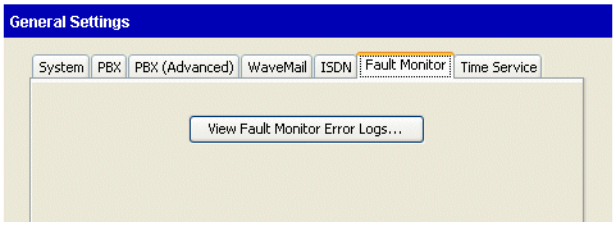
If a bluescreen event occurs, the operating system bluescreen data generated by the event is saved in a memory dump in c:\windows\memory.dmp.

The contents of these buffers are lost if the Wave Server is powered off. In any situation where the Wave is non-responsive and you wish to preserve the contents of these buffers for later access, you should use the black reset button located on the Integrated Services Card. The Wave Server should not be powered off so as to preserve the traces in the fault monitor buffers.

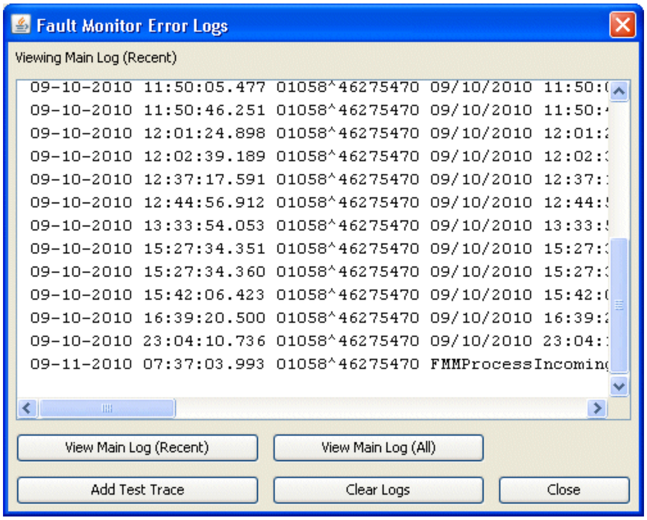
To view the Fault Monitor Error Logs

Click

1. If necessary, click the Administration tab of the Management Console.
2. Click the General Settings icon, located in the General Administration section.
3. Select the Fault Monitor tab.



4. Click **View Fault Monitor Error Logs**.



Viewing Main Log (Recent)

```
09-10-2010 11:50:05.477 01058^46275470 09/10/2010 11:50:0
09-10-2010 11:50:46.251 01058^46275470 09/10/2010 11:50:4
09-10-2010 12:01:24.898 01058^46275470 09/10/2010 12:01:2
09-10-2010 12:02:39.189 01058^46275470 09/10/2010 12:02:3
09-10-2010 12:37:17.591 01058^46275470 09/10/2010 12:37:1
09-10-2010 12:44:56.912 01058^46275470 09/10/2010 12:44:5
09-10-2010 13:33:54.053 01058^46275470 09/10/2010 13:33:5
09-10-2010 15:27:34.351 01058^46275470 09/10/2010 15:27:3
09-10-2010 15:27:34.360 01058^46275470 09/10/2010 15:27:3
09-10-2010 15:42:06.423 01058^46275470 09/10/2010 15:42:0
09-10-2010 16:39:20.500 01058^46275470 09/10/2010 16:39:2
09-10-2010 23:04:10.736 01058^46275470 09/10/2010 23:04:1
09-11-2010 07:37:03.993 01058^46275470 FMMProcessIncomin
```

5 Click one of the following buttons:

- **View Main Log (Recent)**. Displays the contents of the last 4K of the Main Log (default view)
- **View Main Log (All)**. Displays the entire contents of the 32K Main Log
- **Add Test Trace**. Adds a test trace with an appropriate time stamp and the text `Management Console ==> Test trace` to the end of the Main Log. To view the test trace, click either **View Main Log (Recent)** or **View Main Log (All)**.
- **Clear Logs**. Clears the contents of the Main Log and Alternate Log. To verify that the logs have been cleared, click View Main Log (Recent), View Main Log (All), or View Alternate Log

6 Click **Close** to close the dialog and return to the General Settings applet.

7 Click **Apply** to save your changes.

8 Click **Done** to return to the Management Console.

Downloading Wave files

The Download applet is a diagnostic tool that allows you to download files from the Wave Server to your workstation for inspection. Files are downloaded by sending them through FTP to the web browser on your workstation. The browser will prompt you to choose a location to save the files.

Hint: One way to use the Download applet is to gather logs to submit a problem report to your Wave provider. For details, see "Gathering logs to report a Wave problem" on page 22-51.

You can download files from any of the following categories:

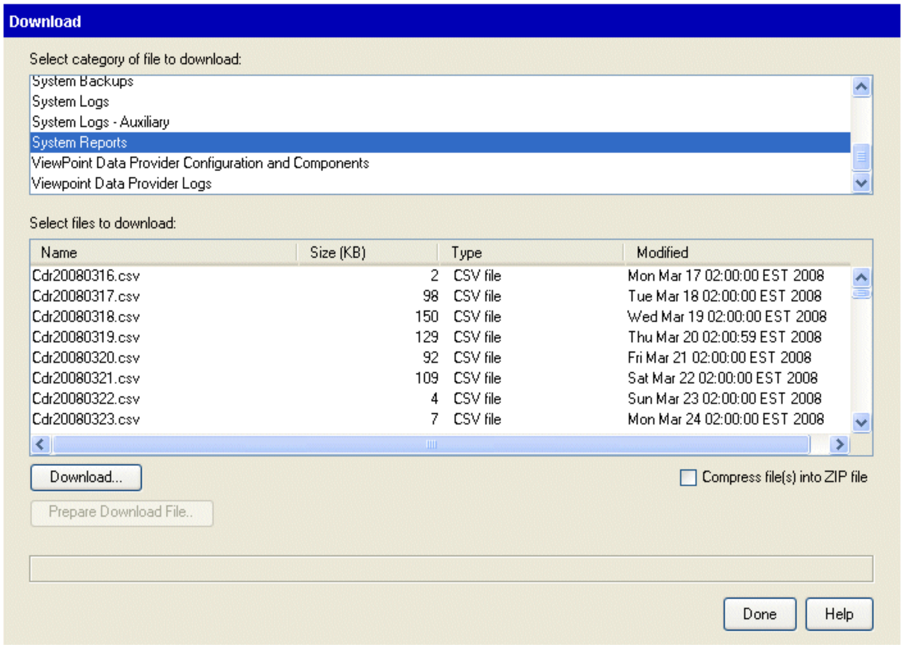
- **CMS Reports**. Reports and log files for Vertical Wave Fax Manager and Vertical Wave Service Response products.
- **CRQ Reports**. Reports and log files for Vertical Wave Fax Manager and Vertical Wave Service Response products.
- **Client Components**. Executables for distribution to client workstations.
- **Call Navigator Reports**. Reports and log files for Call Navigator.
- **Database**.
- **Global Administrator History.** History file for Management Console access.
- **Global Administrator Logs**. Log file for Management Console access.
- **IIS Logs**.
- **Log Bundles**. Log files in this category are used when troubleshooting Wave problems. See "Gathering logs to report a Wave problem" on page 22-51.
- **SQL Server Logs**.
- **System Backups**. Configuration backup CAB files and backup logs.
- **System Logs**. Wave Server logs.
- **System Logs - Auxiliary.** Wave Server auxiliary logs. Log files in this category are used when troubleshooting Wave problems. See "Gathering logs to report a Wave problem" on page 22-51.
- **System Reports**. Daily archives from the Call Detail Report and Trunk Statistics Report.
- **ViewPoint Data Provider Configuration and Components**. Configuration settings for the ViewPoint Data Provider.
- **ViewPoint Data Provider Logs**. Activity history for all ViewPoint database requests.

To download Wave files

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Download icon, located in the General Administration section.



Select category of file to download:

System Backups
System Logs
System Logs - Auxiliary
System Reports
ViewPoint Data Provider Configuration and Components
Viewpoint Data Provider Logs

Select files to download:

Name	Size (KB)	Type	Modified
Cdr20080316.csv	2	CSV file	Mon Mar 17 02:00:00 EST 2008
Cdr20080317.csv	98	CSV file	Tue Mar 18 02:00:00 EST 2008
Cdr20080318.csv	150	CSV file	Wed Mar 19 02:00:00 EST 2008
Cdr20080319.csv	129	CSV file	Thu Mar 20 02:00:59 EST 2008
Cdr20080320.csv	92	CSV file	Fri Mar 21 02:00:00 EST 2008
Cdr20080321.csv	109	CSV file	Sat Mar 22 02:00:00 EST 2008
Cdr20080322.csv	4	CSV file	Sun Mar 23 02:00:00 EST 2008
Cdr20080323.csv	7	CSV file	Mon Mar 24 02:00:00 EST 2008

□ Compress file(s) into ZIP file

3 Select a category from the list at the top of the screen.

4 Select a file or group of files from the file list.

5 Select the **Compress file(s) into ZIP file** check box to compress the files using WinZIP. (If you select more than one file, this option is selected automatically.)

6 Click **Download**.

7 Save the file to your local hard drive.

8 Click **Done** to return to the Management Console.

Setting the minimum free hard drive space notification limit

This option allows you to set a notification to warn you when there is between 50-400 megabytes of primary hard drive space left on your Wave Server.

Note: You must be monitoring your Wave Server with SNMP to benefit from this feature.

To set a minimum free hard drive space notification limit

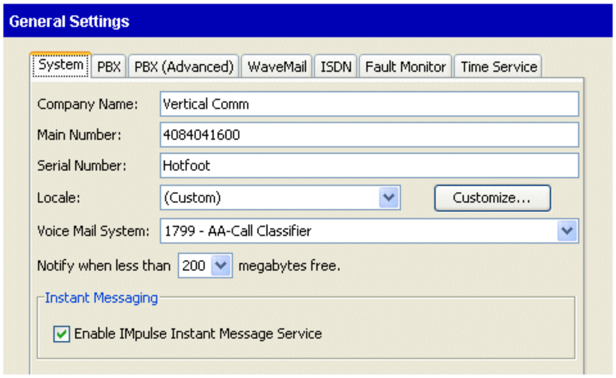
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the System tab.

4 Select a number from the **Notify when less than __ megabytes free** drop-down list.



Company Name: Vertical Comm

Main Number: 4084041600

Serial Number: Hotfoot

Locale: (Custom)

Voice Mail System: 1799 - AA-Call Classifier

Notify when less than 200 megabytes free.

☑ Enable IMpulse Instant Message Service

When your hard drive reaches the limit you set, an SNMP trap will be sent with the following message:

```
Min Free Space=n. Current Avail Free Space=y.
```

where *n* is the amount of minimum memory in megabytes you set, and *y* is the actual current available free space.

5 Click **Apply** to save your changes.

6 Click **Done** to return to the Management Console.

Configuring and using SNMP

Simple Network Management Protocol (SNMP) can be used to monitor and diagnose a Wave Server, notifying you about any alarms and traps.

Using the SNMP Configuration applet, you can configure traps to notify specified clients about any unsolicited events and you can set up several levels of security. Using the SNMP Alarms applet, you can monitor current and review previous alarms. Wave supports the SNMP agents listed in Chapter 32, SNMP Agents.

All Management Information Bases (MIBs) reside on the Wave Server in the `C:\Program Files\SNMP\MIBs` directory.

For complete information about Wave SNMP agents and a list of other supported agents, see:

- SNMP terminology
- Configuring SNMP agents
- Configuring an SNMP trap filter
- Configuring SNMP security
- Configuring a contact
- Using SNMP alarms

SNMP terminology

SNMP terminology used in the configuration applet is explained in the following table.

Term	Meaning
Community Name	Both the SNMP management system and SNMP agent must be members of a group so that SNMP messages can be passed between them. The logical name assigned to such a group can be any combination of alphanumeric characters, and is referred to as a *community name*. SNMP operations require a valid community name; up to seven community names can be specified. Community names, known only to registered users or administrators, provide the security required by SNMP SET operations. The globally known “public” can be used as a community name, but does not provide security. If no community is specified, all SNMP requests will be honored. The SNMP agent residing on the managed node accepts or rejects an SNMP request based on the community name contained in the request. For example, an agent configured with the community name “vertical” rejects all requests containing any other community name.
Host	The management system requesting SNMP information from this Wave Server.
Trap	An unsolicited asynchronous message sent from an SNMP agent to a management system. Traps are typically sent by the agent when a predefined condition or event occurs. For details on such conditions and events, see Chapter 32, SNMP Agents.
Trap Community	The string encoded in a trap message (packet) by the agent; placeholder for trap destinations. Like community name, the trap community name can be any combination of alphanumeric characters; unlike community name, trap community names have nothing to do with security. “Public” is fine to use as a default.
Trap Destination	A specific network address (IP or DNS host name) to which a trap message is sent. Up to five trap destinations can be added for each trap community.

Configuring SNMP agents

You will typically access the SNMP Configuration applet to configure community names, trap destinations, and specific management (host) destinations. Once SNMP agents are configured:

- Users can view SNMP traps from the Wave Server through the SNMP Alarms applet.
- Specified clients will be notified when SNMP traps occur.

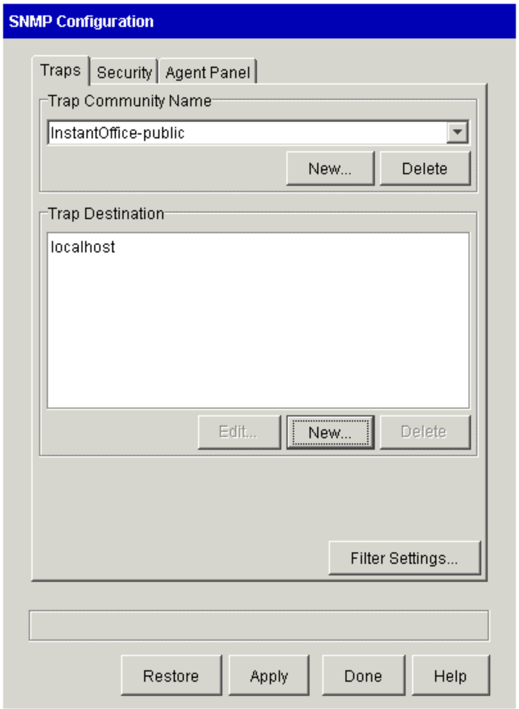
To configure SNMP traps

Click

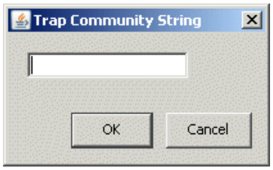
1. If necessary, click the Administration tab of the Management Console.
2. Click the SNMP Configuration icon, located in the General Administration section.
3. On the Agent Panel tab, enter the following information:
    - **Contact**. Enter information about the contact person for this Wave Server.
    - **Location**. Enter information about the physical location of this Wave Server.

   Both fields can contain a maximum of 255 characters.

4 Click the Traps tab.



5 Click **New** to add a trap community name.



6 Type `InstantOffice-public`, and click **OK**.

You must have a valid trap community name in order to see SNMP alarms. Public is the default community string, but it can be changed.

7 Repeat steps 5 and 6 to add more trap community names.

To add a trap destination

1 Choose a trap community name from the list.

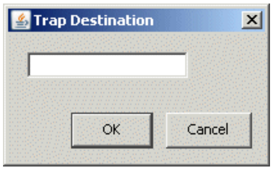
2 Click **New** under Trap Destination. The Trap Destination dialog opens.

3 Type the DNS host name of the Wave Server, and IP address of the trap destination, then click **OK**.

By default, the trap destination list includes localhost, which means that SNMP alarms will be returned to the Wave Server you are configuring, and can be monitored via the SNMP Alarms applet in the Management Console.

4 Repeat to add more trap destinations.

Client machines listed as trap destinations receive SNMP traps, which can be viewed from the SNMP Alarms applet. All client destinations listed as trap destinations receive SNMP traps from this Wave Server. The community name encoded in the trap message depends on which community the trap destination belongs.



Configuring an SNMP trap filter

Using SNMP Filters, you can enable and disable specific groups (trap groups) of SNMP traps to filter the traps for network monitoring tools.

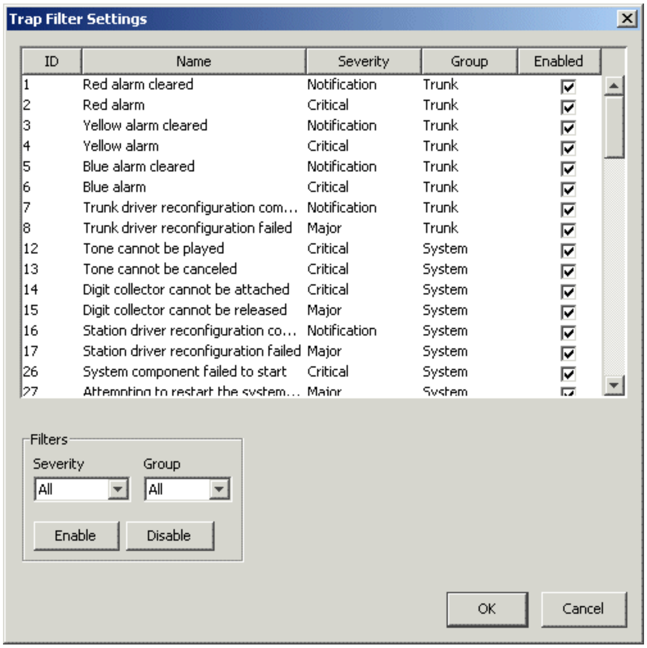
To filter SNMP traps

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Configuration icon, located in the General Administration section.

3 Click the Filter Settings button on the Traps tab.



Trap Filter Settings

ID	Name	Severity	Group	Enabled
1	Red alarm cleared	Notification	Trunk	☑
2	Red alarm	Critical	Trunk	☑
3	Yellow alarm cleared	Notification	Trunk	☑
4	Yellow alarm	Critical	Trunk	☑
5	Blue alarm cleared	Notification	Trunk	☑
6	Blue alarm	Critical	Trunk	☑
7	Trunk driver reconfiguration com...	Notification	Trunk	☑
8	Trunk driver reconfiguration failed	Major	Trunk	☑
12	Tone cannot be played	Critical	System	☑
13	Tone cannot be canceled	Critical	System	☑
14	Digit collector cannot be attached	Critical	System	☑
15	Digit collector cannot be released	Major	System	☑
16	Station driver reconfiguration co...	Notification	System	☑
17	Station driver reconfiguration failed	Major	System	☑
26	System component failed to start	Critical	System	☑
27	Attempting to restart the system...	Major	System	☑

Filters

Severity: All

Group: All

4 You can enable or disable traps by severity or by group using the Severity and Group drop-down lists and clicking Enable or Disable.

You can select All, Critical, Major, or Notification traps in the **Severity** drop-down list.

You can select All, System, Trunk, Upgrade, Hardware, OS, Data, and MSM from the **Group** drop-down list.

For those traps that are selected for filtering, the **Enabled** check box is checked.

5 Click **OK**.

6 Click **Done** to save your changes return to the Management Console.

Configuring SNMP security

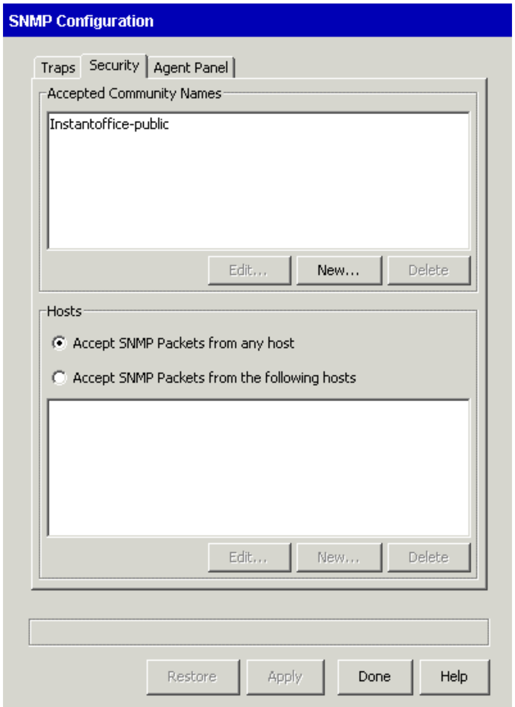
To configure SNMP security

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Configuration icon, located in the General Administration section.

3 Click the Security tab.



Accepted Community Names

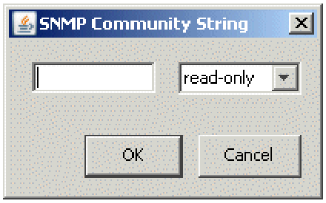
Instantoffice-public

Hosts

● Accept SNMP Packets from any host

○ Accept SNMP Packets from the following hosts

4 Click **New** to add an SNMP community name.



5 Type a valid SNMP community name.

If no community name is specified, SNMP requests containing any community name are accepted. A certain level of security can be effected by setting the agent to allow another private community string. Up to seven such community names can be specified on the agent. SNMP requests will only be accepted if they contain one of the configured community names.

6 Specify if the community string is read-only or read-write using the drop-down list.

7 Click **OK**.

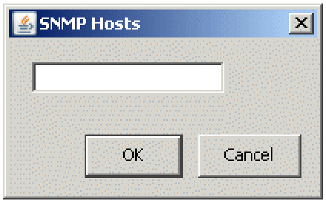
8 Repeat steps 4 through 7 to add more community names.

9 If you wish to specify that SNMP messages be accepted only from particular hosts:

a Click the **Accept SNMP packets only from the followings hosts** option.

b Click **New.**

The SNMP Hosts dialog opens.



c Type the host name or IP address, and click **OK**.

d Repeat to add more hosts.

Naming particular hosts adds another level of security to SNMP monitoring. By default, SNMP packets are accepted from any host.

10 Click **Apply** to save your changes.

11 Click **Done** to return to the Management Console.

Configuring a contact

If you want to specify a person or organization to contact in the case of an SNMP alarm that requires immediate attention, you can enter that information in the Agent Panel tab in the SNMP Configuration applet.

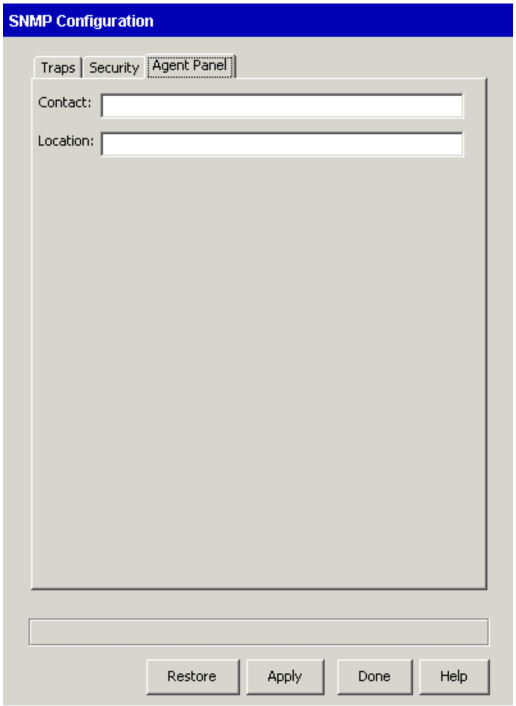
To configure a contact

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Configuration icon, located in the General Administration section.

3 Click the Agent Panel tab.



4 Type the name of the person or organization to contact in the **Contact** field.

5 Type the location, or a phone number, of the person or organization to contact in the **Location** field.

6 Click **Done** to save your changes and return to the Management Console.

Using SNMP alarms

You will access the SNMP Alarms applet frequently as you monitor the Wave Server. Once the SNMP Configuration applet has been configured, the SNMP Alarms applet reports all SNMP traps sent by SNMP agents residing on the Wave Server. You can view alarms to help determine why, for example, your T-1 link or the Wave Server is down.

SNMP alarms can also be sent to third-party monitors by specifying their IP address and setting appropriate community names. Consult your SNMP monitor documentation for further details.

Caution! *You cannot see any SNMP alarms unless trap destinations are configured in the SNMP Configuration applet. You must configure a valid trap community name, and the host name or IP address of the Wave Server as the trap destination.*

The SNMP Alarms applet provides two views:

- Current alarms, the real-time traps occurring in the Wave Server. Once you have noted the trap, you can remove it from this view.
- Previous alarms, those that have occurred when the client was not monitoring alarms in real time. All alarms are retained in a permanent record which you can view at any time by using the Previous Alarms button.

Types and severity of alarms are detailed in Critical Alarms.

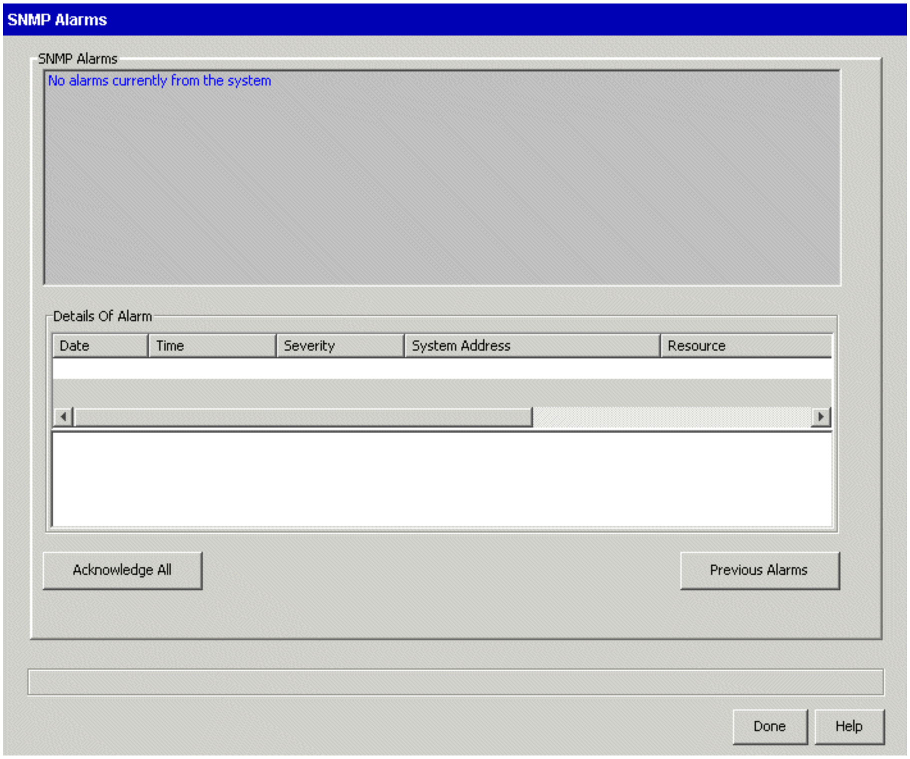
Note: The alarms, **Connection to the system is lost** and **Connection to the system is restored** are not SNMP alarms and the time stamps associated with them are approximate.

To use the SNMP Alarms applet

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Alarms icon, located in the General Administration section.



SNMP Alarms

SNMP Alarms

No alarms currently from the system

Details Of Alarm

Date	Time	Severity	System Address	Resource

The most recent alarms are displayed in the upper list box.

To monitor alarms in real time, leave the applet open. Alarms are reported continuously, since a permanent connection with the Wave Server is maintained.

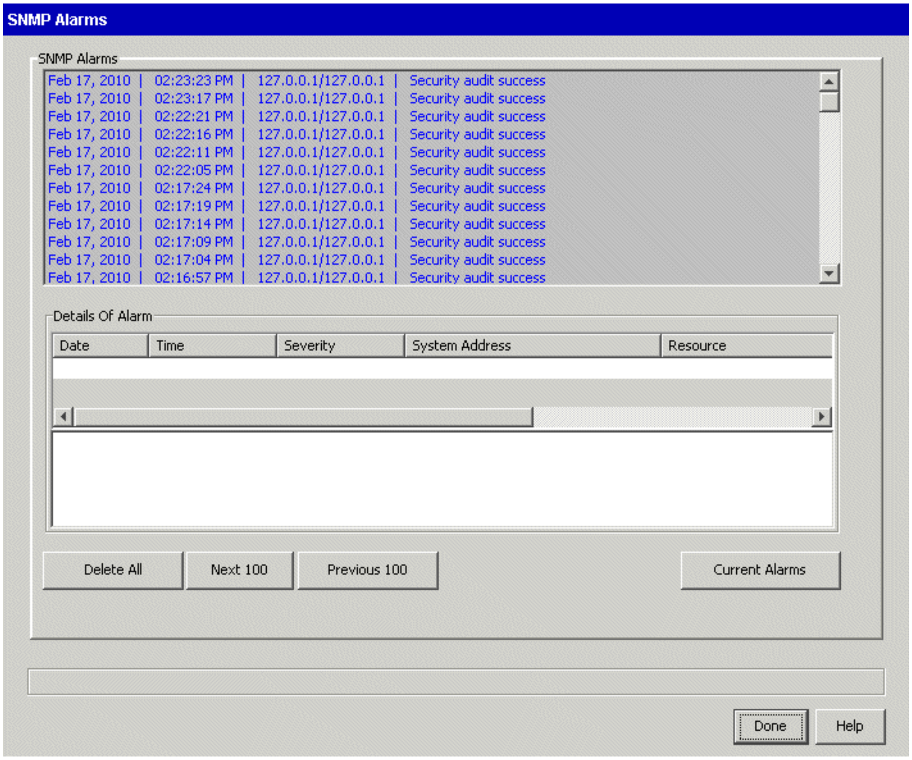
The SNMP Alarms applet displays the most recent alarm at the top of the list.

3 Select an alarm to view details in the lower text area.

4 Click **Acknowledge All** to remove the list of current alarms and place them in the Previous Alarms log.

5 To see a list of all previous alarms, click **Previous Alarms**.

The SNMP Alarms applet displays all the previous Wave alarm messages.



```
Feb 17, 2010 | 02:23:23 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:23:17 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:22:21 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:22:16 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:22:11 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:22:05 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:17:24 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:17:19 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:17:14 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:17:09 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:17:04 PM | 127.0.0.1/127.0.0.1 | Security audit success
Feb 17, 2010 | 02:16:57 PM | 127.0.0.1/127.0.0.1 | Security audit success
```

Date	Time	Severity	System Address	Resource

6. Click **Next 100** or **Previous 100** to traverse through the alarms.
7. Double-click an alarm to display the details for that alarm.
8. Click **Delete All** to remove all the alarms from the Previous Alarms log. This also deletes the history file from the file system.
9. Click **Current Alarms** to return to the applet that lists only the current SNMP alarms.
10. Click **Apply** to save your changes.
11. Click **Done** to return to the Management Console.

Critical Alarms

Most critical (red) alarms are initiated by the Wave Server, although in some cases a service provider’s equipment signal will be displayed as a red alarm. Critical alarms indicate a significant problem with the T-1 link or the Wave Server. Some of the causes for a critical alarm follow.

- Cable is not connected
- Not receiving a T-1 stream because of a short in the RCV wires
- Receiving an incompatible DS1 frame structure
- Receiving signal (voltage) is too weak because the trunk cable is too long

Major Alarms

Most major (yellow) alarms are initiated by your service provider because their equipment is not able to process the T-1 stream. Some of the causes for a major alarm follow:

- Service provider is receiving incompatible DS1 frame structure
- Transmitting signal is too weak because the trunk cable is too long

Notification Alarms

Notification (green) alarms indicate a system modification. For example, a T-1 module or analog station module has been reconfigured.

Using Disk Management and configuring RAID 1

You will typically access the Disk Management application using the RAID 1 Configuration icon to determine the status of your Wave Server hard drives, mirror a new hard drive, or use a mirrored hard drive to recover Wave after a failure. You can also mirror a hard drive as a method of backing up your Wave configuration.

Clearing an old hard drive

To clear an old hard drive

1 Shut down the Wave Server.

2 Insert the old hard drive in slot B.

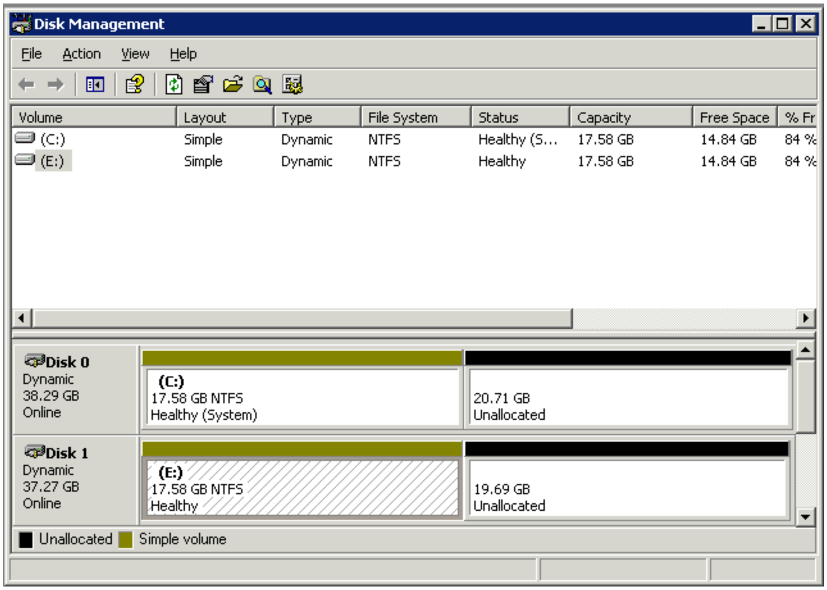
3 Restart the Wave Server.

4 If necessary, click the Administration tab of the Management Console.

Click

5 Click the RAID 1 Configuration icon, located in the General Administration section.

6 Select a partition on Disk 1.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Fr
(C:)	Simple	Dynamic	NTFS	Healthy (S...	17.58 GB	14.84 GB	84 %
(E:)	Simple	Dynamic	NTFS	Healthy	17.58 GB	14.84 GB	84 %

Disk 0 Dynamic 38.29 GB Online	**(C:)** 17.58 GB NTFS Healthy (System)	20.71 GB Unallocated
Disk 1 Dynamic 37.27 GB Online	**(E:)** 17.58 GB NTFS Healthy	19.69 GB Unallocated

■ Unallocated ■ Simple volume

7 Choose **Action > All Tasks > Delete Volume**.

8 Click Yes.

The drive letter will be removed, the partition will be cleared, and a new color will indicate free space (the default is striped).

9 Repeat steps 6 to 8 for each partition.

A hard drive should be free and clear of partitions before it is used for mirroring.

Cloning a hard drive using RAID

Cloning a hard drive, using RAID, is an effective way to create a duplicate of Wave.

To clone a hard drive

1 Create a mirror of the hard drive using the instructions in “Mirroring your hard drive and RAID” on page 15-8.

2 Shut down the Wave Server.

3 Remove the hard drive from Slot B.

4 Restart the Wave Server.

5 If necessary, click the Administration tab of the Management Console.

Click

6 Click the RAID 1 Configuration icon, located in the General Administration section.

7 Select **Action > All Tasks > Remove Mirror**.

8 Select **Disk 1**, then click **Remove Mirror**.

9 Shut down the Wave Server.

10 Insert a new hard drive and restart the Wave Server.

11 Establish the mirror between the two hard drives, using the instructions in “Mirroring your hard drive and RAID” on page 15-8.

12 Install the hard drive you removed in another Wave Server.

You will need to assign new IP addresses and a new host name to the Wave Server housing the cloned hard drive you removed from the original Wave Server.

Identifying RAID disk health

To determine the condition of a mirror set, periodically check the status bar in the Disk Management application. Disk Management displays information about the mirror in the Status column in the Volume List. The following table describes each status type that could be displayed in the Disk Management Status column. If a partition in the set is damaged or loses synchronization with the other partition, FAILED or FAILED REDUNDANCY is displayed.

Status	Description
FAILED	Displayed when a volume cannot be started automatically or the disk is damaged.
FAILED REDUNDANCY	Displayed when one of the mirrored disks is not online.
HEALTHY	Status if the mirror set is healthy.
REGENERATING	Displayed while Wave is generating the mirror set.
RESYNCHING	Displayed while Wave is establishing the mirror.

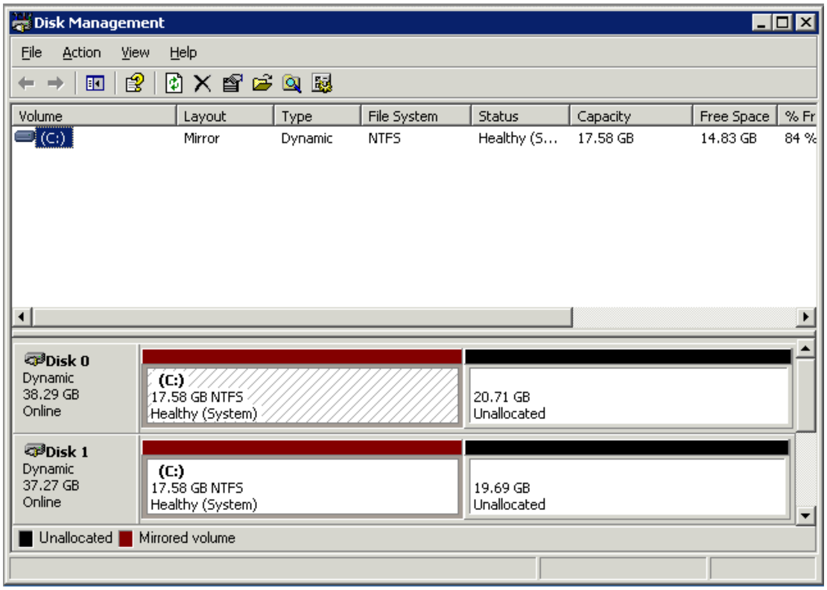
To check the status of a RAID disk

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the RAID 1 Configuration icon, located in the General Administration section.

Mirrored and HEALTHY disks appear like this in the Disk Management applet:



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Fr
(C:)	Mirror	Dynamic	NTFS	Healthy (S...	17.58 GB	14.83 GB	84 %

Disk 0
Dynamic
38.29 GB
Online

(C:)
17.58 GB NTFS
Healthy (System)

20.71 GB
Unallocated

Disk 1
Dynamic
37.27 GB
Online

(C:)
17.58 GB NTFS
Healthy (System)

19.69 GB
Unallocated

■ Unallocated 🟥 Mirrored volume

Recovering with RAID-1 Configuration

If the disk in the Wave Server's slot A is damaged, use the disk in slot B to restart the Wave Server.

Hint: The Windows Event Viewer may help you determine hardware status and what happened to cause the damage.

To recover Wave from a mirrored disk

1 Shut down the Wave Server.

2 Remove the hard drive from slot A.

3 Move the mirrored hard drive from slot B to slot A.

4. Restart the Wave Server.
5. If necessary, click the Administration tab of the Management Console.
6. Click the RAID 1 Configuration icon, located in the General Administration section.

   Click

7. Select **Action > All Tasks > Remove Mirror**.
8. Select Disk 1, then click **Remove Mirror**.

   Note: No fault tolerance is available until a new mirror is established.

9. Re-establish fault tolerance (RAID-1). To do so:
   - **a** Shut down the Wave Server.
   - **b** Insert a new hard drive in slot B.
   - **c** Follow the instructions in “Mirroring your hard drive and RAID” on page 15-8.

Managing Wave system resources

Many Wave and third-party applications require system port DSP resources such as TAPI/WAVE ports, Fax ports, and IP telephony ports. You manage system port DSP resources via the Resource Management applet in the Global Administrator. The type and number of system ports available on your Wave Server may vary depending on which cards and modules that are installed. For information about the resources included on your Wave Server cards and modules, refer to the *Wave Server Hardware Reference Guide*.

Caution! *You must allocate an appropriate number of resources to cover your system demand. If you under-allocate resources, calls may be lost or not handled as expected.*

Determining how many system resources are required

There are two ways to determine how many and what type of system resources you need to allocate to meet your system's requirements:

- **Use the Resource Management Advisor.** The Resource Manager Advisor asks you a series of questions, for example how many analog, digital and SIP phones will be connected, how many simultaneous calls need to be supported, and so forth. Based on your answers and the cards, modules, and Wave licenses installed on your Wave Server, the Resource Manager Advisor then lists the recommended resources that need to be allocated to support the requirements (phone, trunk, conference, call recording, and so forth) that you specified. The Resource Management Advisor is ideal for Wave system administrators who are relatively unfamiliar with the Wave ISM platform, or who want to quickly determine the resources required.

  The Resource Management Advisor calculates requirements for most resource types, including:

  - Phones
  - Call recording
  - Trunks
  - Conferencing
  - Music On Hold

- Voice Mail
- Call Volume
- Contact Center
- Fax Manager

If you need to support additional applications or features (see the table on page 23-50), you must identify the required resource types and then manually calculate and allocate the number of each type that you require to support your needs.

- **Manually calculate the resources of each type that you require to meet your needs** (see the table on page 23-50) , factoring in both the hardware and Wave licenses installed on your Wave Server, as well as other system resource limits described on page 23-53. (Note that the installed hardware, licenses, and resource limits are factored in automatically if you use the Resource Management Advisor.)

Resource requirements for transitory events

Some Voice Over IP DSP resources are used only briefly during the life a of a call or while a feature is being used. To avoid problems (such as no ring back on calls), you must allocate sufficient Voice Over IP DSP resources so that additional resources are available beyond the number required to support the total concurrent IP calls that you require.

Important! In this version, you must allocate these additional resources manually, even if you are using the Resource Manager Advisor—the current resource calculation algorithm used by the Resource Manager Advisor does not allocate them automatically.

Additional Voice Over IP DSP resource will be required in the following call scenarios.

- When all digits are not dialed before placing a call from a SIP phone, an additional DSP resource will be required to apply fast busy tone in case of an inter-digit timeout or call failure, or to apply ringback tone on a successful call.
- When a VoIP call is placed using Viewpoint, an additional DSP resource will be required to apply ringback tone on a successful call.
- For any feature invoked from a SIP phone either via a Feature button or by pressing Flash followed by a * code, an additional DSP resource will be required to apply dial or stutter dial tone.
- When a SIP Phone or SIP trunk is involved in a blind transfer, an additional DSP resource will be required to apply ringback tone.

Using the Resource Management applet and Resource Management Advisor

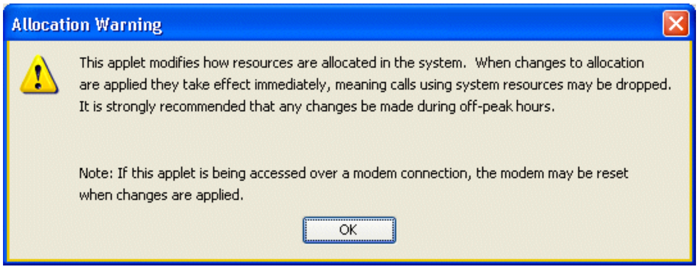
To add, change, or remove system resources

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Resource Management icon, located in the PBX Administration section.

When you start the Resource Management applet, the following message is displayed to remind you to schedule your updates carefully to avoid disrupting your phone service:



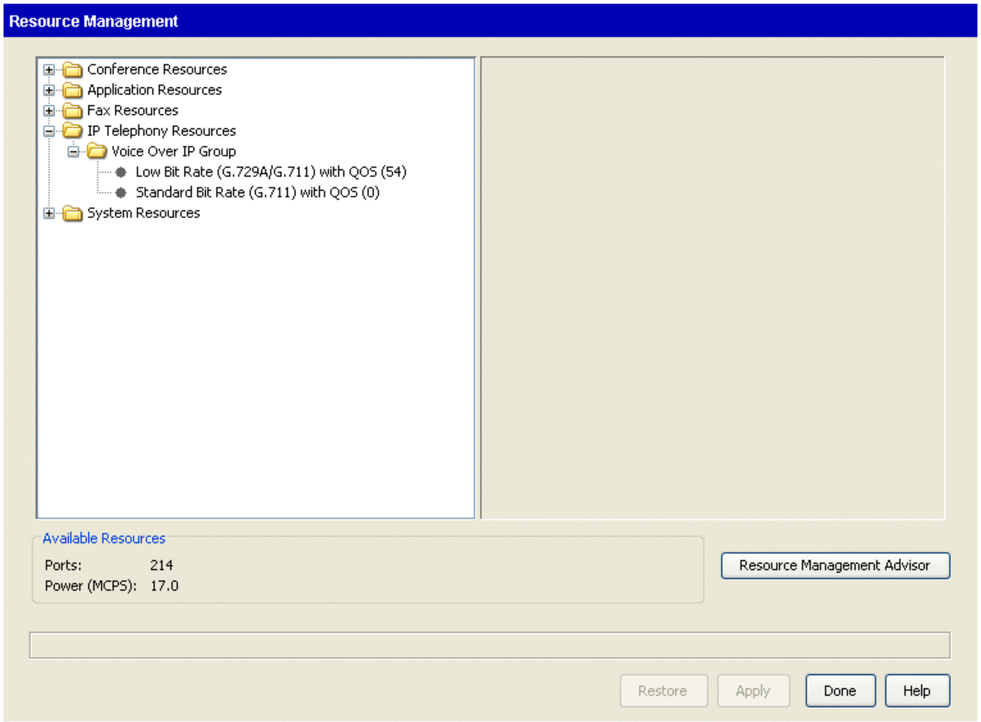
Allocation Warning

This applet modifies how resources are allocated in the system. When changes to allocation are applied they take effect immediately, meaning calls using system resources may be dropped. It is strongly recommended that any changes be made during off-peak hours.

Note: If this applet is being accessed over a modem connection, the modem may be reset when changes are applied.

Click **OK** to continue.

3 When the Resource Management applet opens, expand any of the groups in the left pane to view the resource types in that group.



Resource Management

- Conference Resources
- Application Resources
- Fax Resources
- IP Telephony Resources
  - Voice Over IP Group
    - Low Bit Rate (G.729A/G.711) with QOS (54)
    - Standard Bit Rate (G.711) with QOS (0)
- System Resources

Available Resources

Ports: 214
Power (MCPS): 17.0

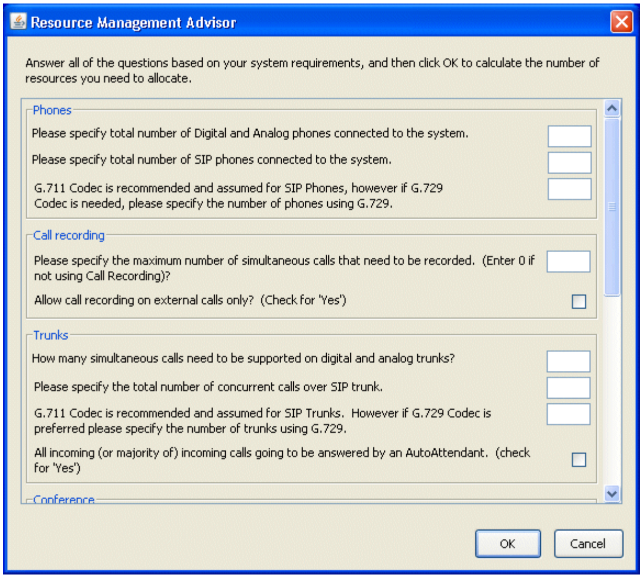
The number in parentheses next to a resource type indicates the number of resources currently allocated.

The **Available Resources** section at the bottom of the dialog shows the number of ports and MCPS (DSP cycles) available. Some resources consume more MCPS than others, so watch both numbers as you change resource allocations. For a description of each resource type, see the table in “System resource types” on page 23-50.

4 Do one of the following:

- If you want Wave to automatically calculate the resources you require, click **Resource Management Advisor**.
- If you already know how many resources you want to allocate, go to step 8.

5 The Resource Management Advisor starts.



Resource Management Advisor

Answer all of the questions based on your system requirements, and then click OK to calculate the number of resources you need to allocate.

Phones

Please specify total number of Digital and Analog phones connected to the system.

Please specify total number of SIP phones connected to the system.

G.711 Codec is recommended and assumed for SIP Phones, however if G.729 Codec is needed, please specify the number of phones using G.729.

Call recording

Please specify the maximum number of simultaneous calls that need to be recorded. (Enter 0 if not using Call Recording)?

Allow call recording on external calls only? (Check for 'Yes') □

Trunks

How many simultaneous calls need to be supported on digital and analog trunks?

Please specify the total number of concurrent calls over SIP trunk.

G.711 Codec is recommended and assumed for SIP Trunks. However if G.729 Codec is preferred please specify the number of trunks using G.729.

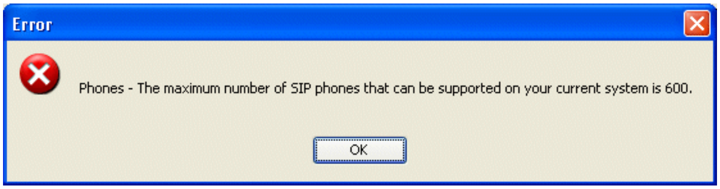
All incoming (or majority of) incoming calls going to be answered by an AutoAttendant. (check for 'Yes') □

Conference

Answer all of the questions. and then click **OK**.

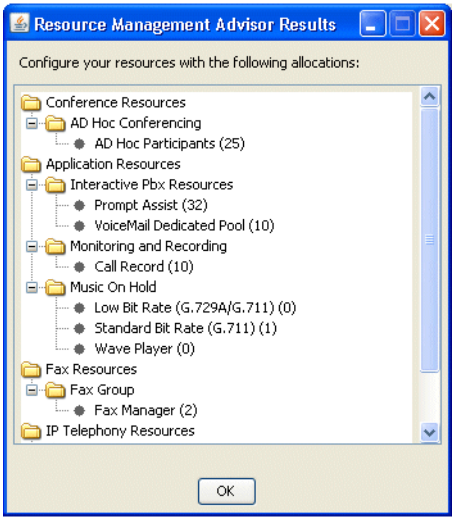
Note the following:

- You must answer every question.
- If the answer to a question is zero, enter “0”—do not leave any answer box blank.
- Based on your answers, the cards, modules, and Wave licenses installed on your Wave Server, as well as other system resource limits, you may see one or more error messages like the following. If you do, go back and enter a lower value for that question and click **OK** again to recalculate:


Error

Phones - The maximum number of SIP phones that can be supported on your current system is 600.

6 When the number of resources required has been successfully calculated, the results are displayed:


Resource Management Advisor Results

Configure your resources with the following allocations:

- Conference Resources
  - AD Hoc Conferencing
    - AD Hoc Participants (25)
- Application Resources
  - Interactive Pbx Resources
    - Prompt Assist (32)
    - VoiceMail Dedicated Pool (10)
  - Monitoring and Recording
    - Call Record (10)
  - Music On Hold
    - Low Bit Rate (G.729A/G.711) (0)
    - Standard Bit Rate (G.711) (1)
    - Wave Player (0)
- Fax Resources
  - Fax Group
    - Fax Manager (2)
- IP Telephony Resources

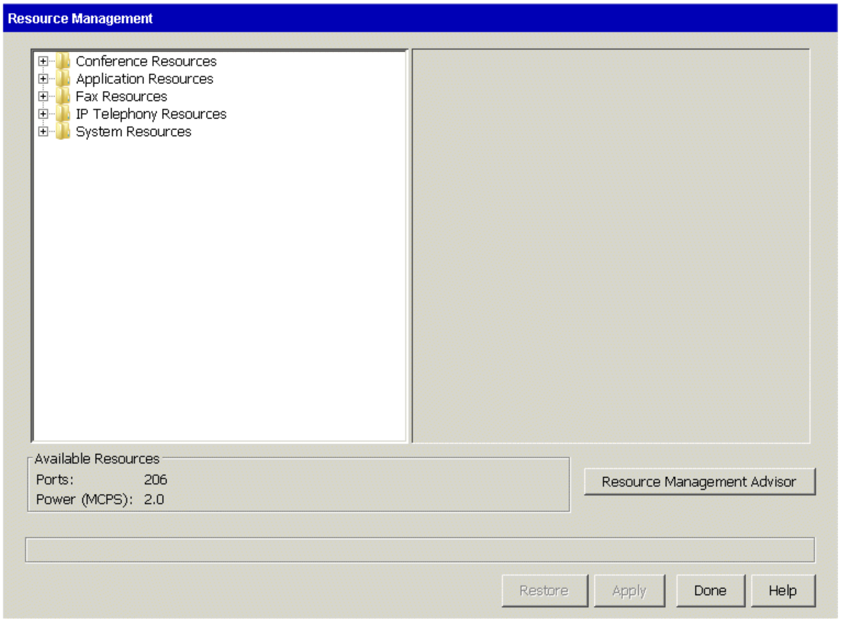
Once you click **OK**, the dialog will close and the information will be lost. To retain the information, do one of the following:

- Make a note of the information or capture a screenshot of the Results dialog before clicking **OK**.
- Leave the Results dialog open and press Alt-Tab as needed to bring the dialog forward again as you allocate the resources.

- Resize the dialogs so that they are open side by side while you allocate the resources.

Make a note of the information in the Results dialog before clicking **OK**, which will close the window. Or, leave the window open and press Alt-Tab as needed to bring the Results dialog forward again as you allocate the resources.

7 Click **OK** in the Resource Management Advisor to return to the Resource Management applet.



Available Resources
Ports: 206
Power (MCPS): 2.0

8 Click an item in the left pane to adjust the number of resources allocated to it in the right pane. The **Available Resources** section at the bottom of the dialog shows the number of ports and MCPS (DSP cycles) available. Some resources consume more MCPS than others, so watch both numbers as you change resource allocations. For a description of each resource type, see the table in “System resource types” on page 23-50.

9 Click **Done** when you are finished.

System resource types

The following table describes the various resources listed in the Resource Management applet. See the appropriate sections in this book or other documentation referenced, for information about allocating resources for the following applications.

Resource	Description
CONFERENCE RESOURCES	
All Conferencing	**Participants**. Used for: • Ad-hoc conference participants, and conference features invoked from a phone or ViewPoint, for example when initiating a conference call and adding parties. • MeetMe conferencing. Conference resources will be made available for MeetMe and ad-hoc conference requests on a first-come, first-served basis—all conferences are treated equally when requesting available conference resources, so be sure to allocate enough conference resources for your specific needs.
APPLICATION RESOURCES	
Interactive PBX Resources	**Plugins**. *This feature is not supported in this version.*
	Prompt Assist. Used to provide IVR functionality to users, for example auto attendants, phone command menu on analog phones, prompts and calls handled via a personal routing list, Contact Center queues, and so forth.

Resource	Description
You can allocate either of the following resource types to support voice mail access. These two resource types are mutually exclusive, so all voice mail resources must be assigned to one option or the other.	
	Voice Mail Dedicated Pool. Used for voicemail access, either a caller leaving a voice message or a user playing back a voice message.
	Voice Mail w/Automatic Gain Control. Same as the previous resource type, but also provides automatic gain control (AGC) for voice mail recordings. (AGC adjusts the volume level of audio as a voice message is recorded so that the playback level is more consistent.).
	Note the following: • Since **Voice Mail w/Automatic Gain Control** resources require more DSP cycles (approximately 30% per resource) than **Voice Mail Dedicated Pool** resources, Vertical recommends that you start out using **Voice Mail Dedicated Pool** resources, and only change to **Voice Mail w/Automatic Gain Control** resources if you encounter too much volume variation during voice message playback. • These two resource types are dedicated for Voice Mail only. Wave will utilize this pool to satisfy voice mail request, however if the pool is empty or all voice mail resources are in use, Wave will make a best effort to utilize Prompt Assist resources to satisfy new voice mail requests.
Monitoring and Recording	**Call Record**. Used for recording calls: • Two Call Record resources are required for each user-to-user call recording session. • When recording conference calls, no additional Call Record resources are needed, no matter how many parties are in the call. See “Allocating DSP resources for call recordings” on page 19-7for more information. Note the following: • **If you enable system call recording**, automatic reallocation of Call Record resources may occur when you log into Wave, as described in “Allocating DSP resources for call recordings” on page 19-7. • **If you do not enable system call recording**, but allow user or queue call recording, automatic reallocation of Call Record resources will not occur, and *call recording may fail if adequate resources are not available*. You must allocate adequate Call Record resources manually via the Resource Management applet if you support user or queue call recording, but not system call recording.

Resource	Description
Call Navigator	Used for sessions of the separate Call Navigator application. The IVR resources cover only IVR used by that application, for example automatic call answering. See the *Wave Call Navigator Administrator Guide* for more information about how to use these resource types.
Service Response	Used for sessions of the separate Service Response application. See the documentation included with Service Response for more information about how to use these resource types.
Voice Server	Used for Wave IVR, for example touchtone button pushes. If your system uses voice recognition, choose "IVR with Voice Recognition" resources. Otherwise choose the standard "IVR" resources. There is normally no need to use both.
Third Party Applications	*This feature is not supported in this version.*
Music on Hold	**Wave Player.** Used to play music-on-hold from WAV files only, not for hold music derived from an external device. See "Configuring Music On Hold" on page 16-21.
	Low Bit Rate (G.729A/G.711). Low bit rate music on hold resources are recommended. Low bit rate resources are *required* if IP calls are expected to use the G729 codec. If IP calls are expected to use the G729 codec and no low bit rate resources are allocated for music on hold, IP callers on hold will hear silence instead of music.
	Standard Bit Rate (G.711).
FAX RESOURCES	
Fax Group	**Fax Manager**. One Fax Manager resource is required for each fax port.
IP TELEPHONY RESOURCES	
Voice Over IP Group	See "Allocating IP telephony resources" on page 6-2. Note that Low Bit Rate codecs use more resources. You must have MRM resources available to use QOS codecs.
	Low Bit Rate (G.729A/G.711) with QOS
	Standard Bit Rate (G.711) with QOS

Resource	Description
SYSTEM RESOURCES	
Detection/Generation	These resources should only be adjusted by advanced users or if you are directed to do so by your Wave technical support representative.
	Caller ID. Used for Caller ID detection and generation. By default, the **Use Automatic Port Allocation** checkbox is selected, meaning Wave automatically allocates resources for optimal performance based on your system's trunks and phones.
	DTMF
	Tone

System resource assignment limits

The Resource Management applet enforces limits on the number of resources that can be assigned to each application.

- **Voice Over IP**. Purchased software licenses allow you to use the DSPs available on the Wave Integrated Services Card for IP telephony. See Chapter 28, DSP resources and licensing for IP telephony resources for more information.
- **Voice Mail**. Limited by sub-group.
- **Call Navigator**. For system resource assignment limits for this application, please see the *Wave Call Navigator Administrator Guide* for more information.
- **Third Party Applications**. Limited to 100 ports.
- **Music On Hold**. 8 ports maximum.
- **Service Response**. For system resource assignment limits for this application, please see its accompanying documentation for more information.
- **Voice Server**. For system resource assignment limits for this application, please see its accompanying documentation for more information.

Note: Some resources are restricted by licenses. If a category requires a license, such as Call Navigator, you will not be able to assign any resources to it until you have entered a valid license key in the Software Licenses applet. See "About Wave licenses" on page 24-2 for more information.

Importing and exporting Wave items

Import/Export provides Wave dealers and administrators with a powerful tool to reduce system administration effort and cost via offline editing of Wave component settings and batch updates, as well as speed up the system staging, installation, deployment, and migration process.

In this version, you can import and export the following ViewPoint components:

- Personal call rules
- Personal routing lists
- Personal routing list actions

Note the following restrictions in this version:

- Importing and exporting a call rule that contains a schedule condition of **During custom hours** is not supported.
- Importing and exporting the Standard routing list (the default routing list that is built into Wave) is not supported.

In future versions, Import/Export will be expanded to support other Wave and ViewPoint components.

Import and export are two distinct features that work hand in hand:

- Export allows you to select one or more components of an existing Wave system and create a set of human-readable and editable files (in CSV, XML or text format) containing data and settings associated with those components. The files follow a published format that is forward-compatible.

  You can use desktop tools (such as Microsoft Excel) to rapidly process the files and change attributes via find/replace, copy/paste, and other data manipulation methods without having to edit specific components and update component settings individually via the Global Administrator Management Console.
- Import uses the data and settings in properly-prepared CSV, XML or text files to update the Wave system configuration in batch mode.

Some ways to use Import/Export include:

- **Simplifying the system staging process**. Configure a Wave system based on the organization’s standard conventions and practices and then export the configuration bundle as a customized “base configuration”. Importing the base configuration quickly stages a new system before any further site-specific customization is performed.
- **Reducing overall labor costs for system updates**. Create template import files and directly delegate site-specific data entry of component information to customers or lower-cost data entry resources.
- **Speeding up new system deployment**. Speed up new system installations or ongoing bulk configuration changes by first exporting the relevant data and then using desktop tools to modify it as needed. The modified file can then be imported to either configure a new system, or update an existing system in a fast, bulk-change mode.
- **Simplifying migration to Wave from other PBXs**. Use data extracted from other PBXs to create import files to bulk provision component information on the new Wave system. (The level of potential automation will depend on the ability of the other PBX to generate the raw data.)

For more information, see:

- Importing Wave components from a file. See page 23-57.
- Exporting Wave components to a CSV file. See page 23-55.

Exporting Wave components to a CSV file

Each exported component is saved as an individual CSV file placed in a ZIP file called WaveExportData.zip. Exported CSV files have the following names:

- PersonalCallRules.csv
- PersonalRoutingList.csv
- PersonalRoutingListActions.csv

See “File formats for importing and exporting” on page 23-61 for more about the format of the exported file.

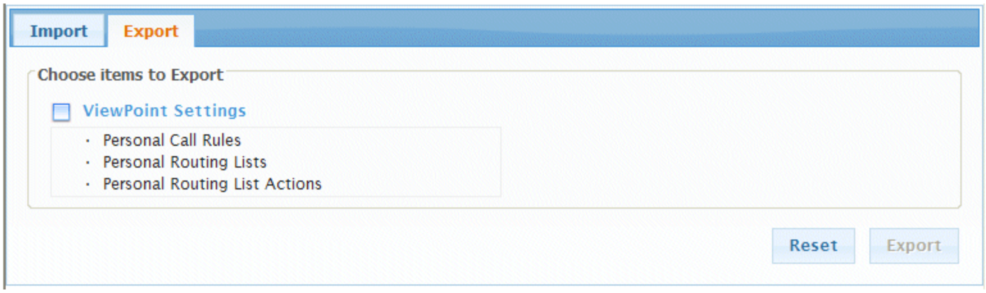
To export Wave components to a CSV file

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Import/Export icon, located in the General Administration section.

3 Click the Export tab.



Import | Export

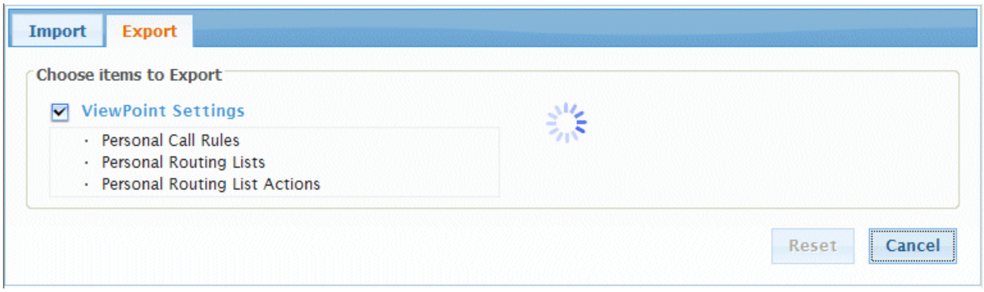
Choose items to Export

□ ViewPoint Settings

- Personal Call Rules
- Personal Routing Lists
- Personal Routing List Actions

4 Select the **ViewPoint Settings** checkbox to export personal call rules, personal routing lists, and personal routing list actions.

5 Click **Export** to continue. (Click **Reset** to deselect all options to re-specify the items to export—the **Reset** button will be disabled once the export starts.)



Import | Export

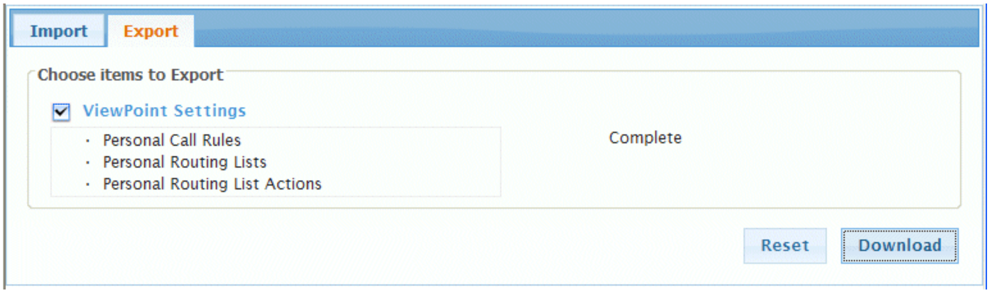
Choose items to Export

☑ ViewPoint Settings

- Personal Call Rules
- Personal Routing Lists
- Personal Routing List Actions

A progress indicator is displayed next to each item that you selected to export. Click **Cancel** at any time to stop the export.

6 When the export completes, click **Download** to create the individual CSV files and the output ZIP file.



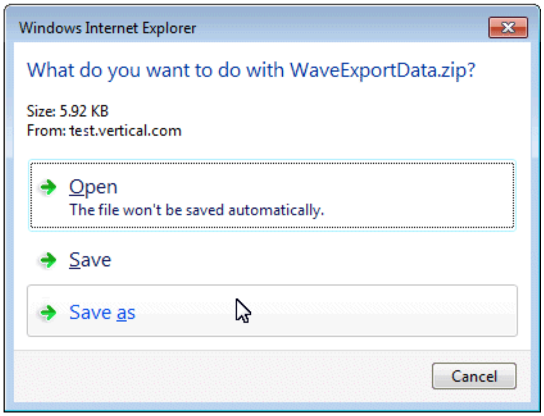
Choose items to Export

☑ ViewPoint Settings

- Personal Call Rules
- Personal Routing Lists
- Personal Routing List Actions

Complete

7 At the prompt, open or save the ZIP file.



What do you want to do with WaveExportData.zip?

Size: 5.92 KB
From: test.vertical.com

Open
The file won't be saved automatically.

Importing Wave components from a file

You can import Wave components from a previously exported file or a file that you have prepared using Microsoft Excel or a text editor like Notepad. You can import all of the files in a ZIP file exported previously, or an individual file or files in the ZIP file. You can also selectively import one or more rows from a file, or make changes to the data in a file before importing.

When you select a file to import as described below, the file is copied to the Wave Server. This copy is deleted when the import completes, or after a predetermined session timeout.

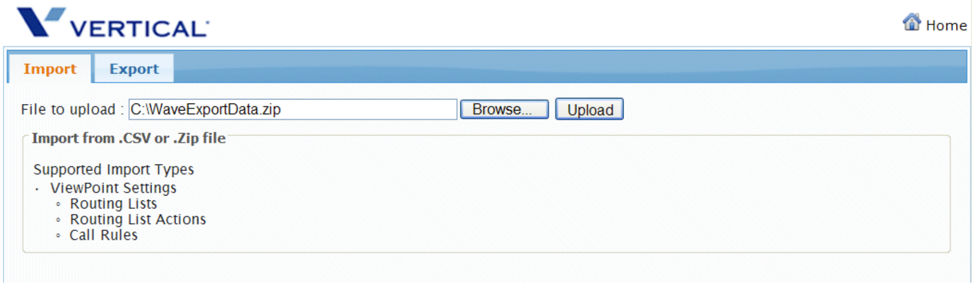
To import Wave components from a file

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Import/Export icon, located in the General Administration section.

3 On the Import tab, browse to the ZIP or individual file that you want to import, and then click **Upload**.

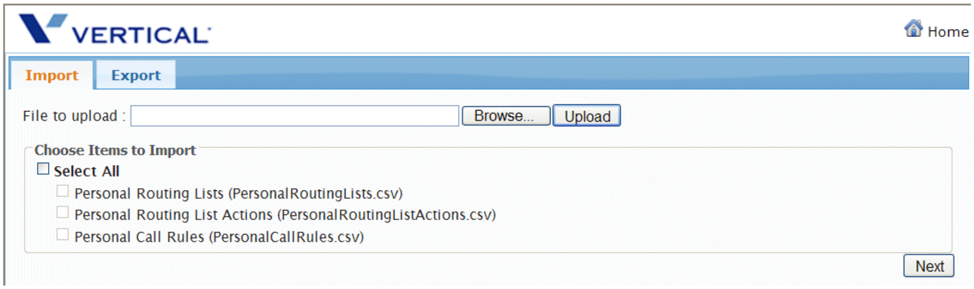


File to upload : C:\WaveExportData.zip

Import from .CSV or .Zip file

Supported Import Types
- ViewPoint Settings
  - Routing Lists
  - Routing List Actions
  - Call Rules

4 Select the components to import.



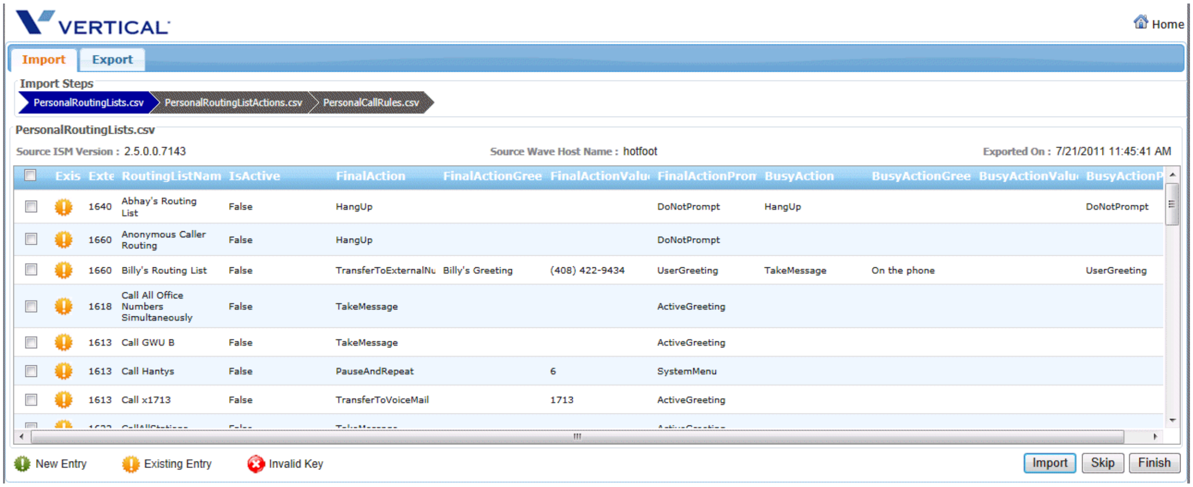
File to upload :

Choose Items to Import
☐ Select All
☐ Personal Routing Lists (PersonalRoutingLists.csv)
☐ Personal Routing List Actions (PersonalRoutingListActions.csv)
☐ Personal Call Rules (PersonalCallRules.csv)

- **Select All**. Selecting this checkbox selects all of the following checkboxes.
  - **Personal Routing Lists**.
  - **Personal Routing List Actions**.
  - **Personal Call Rules**.

Click **Next** to continue.

5 The contents of the file (or the first file in a ZIP file) are displayed.



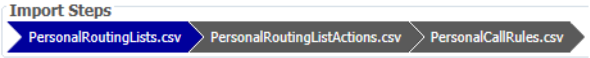
PersonalRoutingLists.csv

Source ISM Version : 2.5.0.0.7143 Source Wave Host Name : hotfoot Exported On : 7/21/2011 11:45:41 AM

☐	Exis	Exte	RoutingListNam	IsActive	FinalAction	FinalActionGree	FinalActionValu	FinalActionPron	BusyAction	BusyActionGree	BusyActionValu	BusyActionP
☐	!	1640	Abhay's Routing List	False	HangUp			DoNotPrompt	HangUp			DoNotPrompt
☐	!	1660	Anonymous Caller Routing	False	HangUp			DoNotPrompt				
☐	!	1660	Billy's Routing List	False	TransferToExternalNu	Billy's Greeting	(408) 422-9434	UserGreeting	TakeMessage	On the phone		UserGreeting
☐	!	1618	Call All Office Numbers Simultaneously	False	TakeMessage			ActiveGreeting				
☐	!	1613	Call GWU B	False	TakeMessage			ActiveGreeting				
☐	!	1613	Call Hantys	False	PauseAndRepeat		6	SystemMenu				
☐	!	1613	Call x1713	False	TransferToVoiceMail		1713	ActiveGreeting				

New Entry ! Existing Entry ✕ Invalid Key

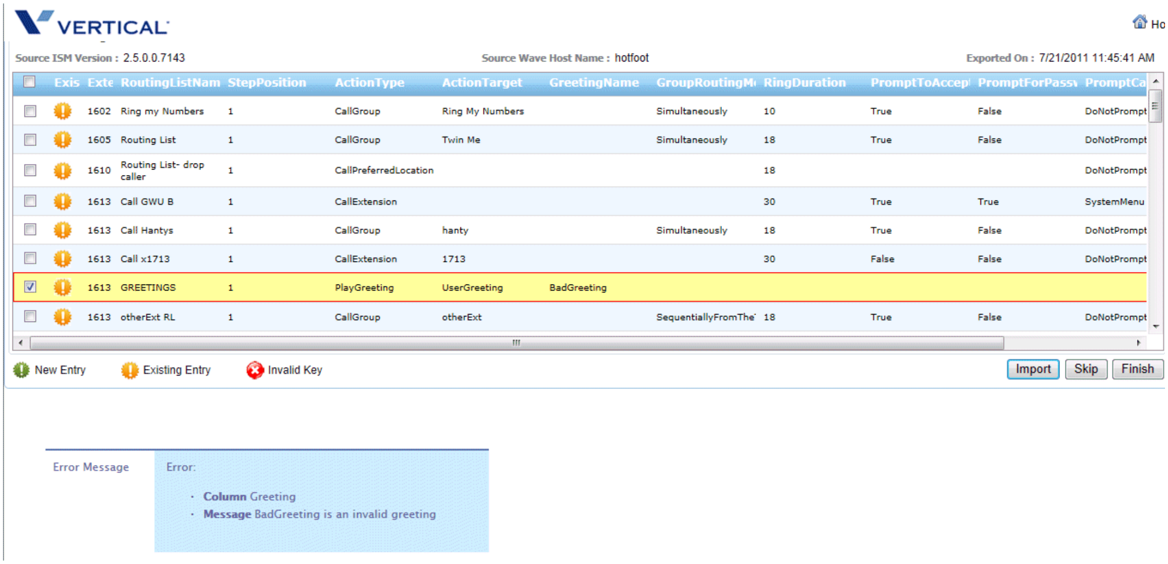
When you select a ZIP file, the individual files are listed under **Import Steps** at the top of the screen:



The filename’s color indicates its status:

- **Blue**. Current file—the contents of each row in this file are listed on the Import tab.
- **Green**. File has been processed, and is ready to be imported.
- **Red**. File has been skipped. Its contents will not be imported.

6 Click on a row to make changes. Note that not all columns can be edited. If you enter invalid data in a column, that error is flagged in yellow. Scroll down to view error message details.



Source ISM Version : 2.5.0.0.7143   Source Wave Host Name : hotfoot   Exported On : 7/21/2011 11:45:41 AM

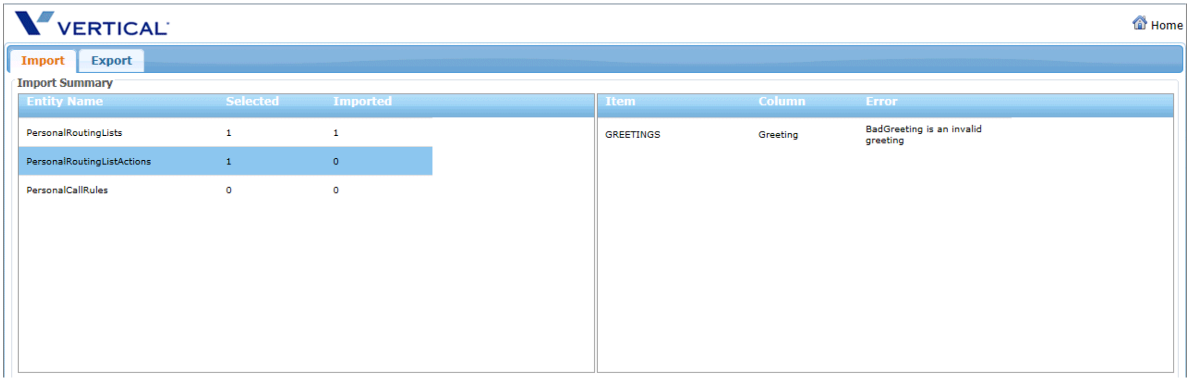
□	Exis	Exte	RoutingListNam	StepPosition	ActionType	ActionTarget	GreetingName	GroupRoutingM	RingDuration	PromptToAccep	PromptForPassv	PromptCa
□	!	1602	Ring my Numbers	1	CallGroup	Ring My Numbers		Simultaneously	10	True	False	DoNotPrompt
□	!	1605	Routing List	1	CallGroup	Twin Me		Simultaneously	18	True	False	DoNotPrompt
□	!	1610	Routing List- drop caller	1	CallPreferredLocation				18			DoNotPrompt
□	!	1613	Call GWU B	1	CallExtension				30	True	True	SystemMenu
□	!	1613	Call Hantys	1	CallGroup	hanty		Simultaneously	18	True	False	DoNotPrompt
□	!	1613	Call x1713	1	CallExtension	1713			30	False	False	DoNotPrompt
☑	!	1613	GREETINGS	1	PlayGreeting	UserGreeting	BadGreeting					
□	!	1613	otherExt RL	1	CallGroup	otherExt		SequentiallyFromThe	18	True	False	DoNotPrompt

Error Message   Error:

- **Column** Greeting
- **Message** BadGreeting is an invalid greeting

7 When you are done editing a file, click **Import** to go to the next file. Click **Skip** to skip any errors in the current file, which will not be included in the import.

8 When you are ready to import, click **Finish**. The results of the import are displayed in the Import Summary.



Import Summary

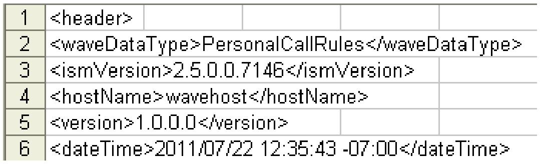
Entity Name	Selected	Imported
PersonalRoutingLists	1	1
PersonalRoutingListActions	1	0
PersonalCallRules	0	0

Item	Column	Error
GREETINGS	Greeting	BadGreeting is an invalid greeting

File formats for importing and exporting

Export file formats

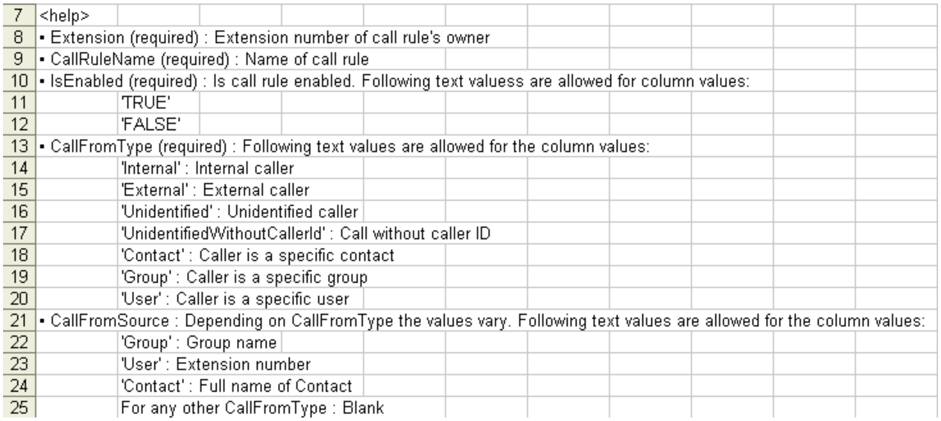
Each exported CSV file contains data specific to the exported item, but all CSV files have a header record in the following format. This example shows the file header for a PersonalCallRules.csv file as viewed in Microsoft Excel.



1	<header>
2	<waveDataType>PersonalCallRules</waveDataType>
3	<ismVersion>2.5.0.0.7146</ismVersion>
4	<hostName>wavehost</hostName>
5	<version>1.0.0.0</version>
6	<dateTime>2011/07/22 12:35:43 -07:00</dateTime>

Preparing a file for import

In an exported file, the <Help> section at the end of the file header lists and describes each column in that file's rows, including all valid entries for each column. This example shows the start of the <Help> section for a PersonalCallRules.csv file as viewed in Microsoft Excel.



7	<help>	
8	▪ Extension (required) : Extension number of call rule's owner	
9	▪ CallRuleName (required) : Name of call rule	
10	▪ IsEnabled (required) : Is call rule enabled. Following text valuess are allowed for column values:	
11		'TRUE'
12		'FALSE'
13	▪ CallFromType (required) : Following text values are allowed for the column values:	
14		'Internal' : Internal caller
15		'External' : External caller
16		'Unidentified' : Unidentified caller
17		'UnidentifiedWithoutCallerId' : Call without caller ID
18		'Contact' : Caller is a specific contact
19		'Group' : Caller is a specific group
20		'User' : Caller is a specific user
21	▪ CallFromSource : Depending on CallFromType the values vary. Following text values are allowed for the column values:	
22		'Group' : Group name
23		'User' : Extension number
24		'Contact' : Full name of Contact
25		For any other CallFromType : Blank

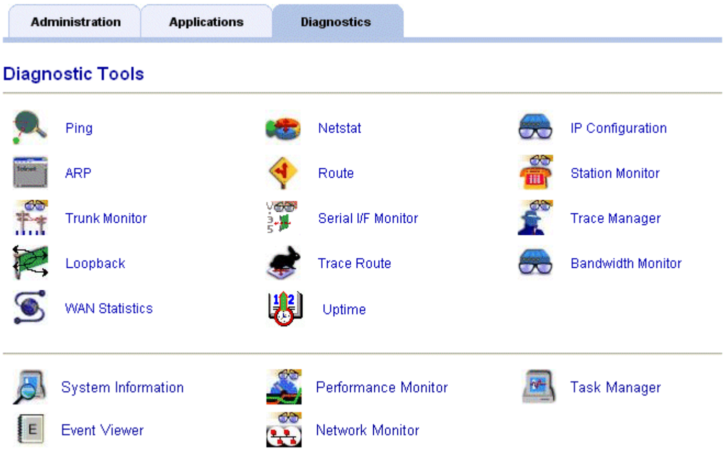
You can use the <Help> section in an exported file as a guide when creating your own file for import from scratch as described below, or to modify a previously-exported file using Microsoft Excel or a text editor such as Notepad.

To create a file for importing

1. In Microsoft Excel or a text editor such as Notepad, create a new file.
2. Add the file header information shown above as the first rows in the file.
3. Add each item (call rule, routing list, and so forth) to be imported as a separate row, and enter the appropriate information for each column.
4. Save the file as a CSV, EML, or text file to any location.

Accessing Diagnostic Tools

Open the Wave Diagnostic Tools console when you need to troubleshoot Wave problems. The Diagnostic Tools console provides access to Wave PBX, voicemail, networking, and Microsoft Windows troubleshooting tools through a Web browser interface. To access the Wave diagnostic tools select the Diagnostics tab from the Management Console.



For information on using the diagnostic tools, click the Help button on each Diagnostic applet, or click the Help icon on the Diagnostic Tools console. The Uptime utility is also documented in the next section.

Using the Uptime utility

Microsoft's Uptime is the Windows Server 2003 utility that allows you to estimate server availability. Uptime processes the machine's event log to determine system availability and current uptime. The target system can either be the local system or a remote system.

Note: Many factors affect Uptime's calculations, and the results displayed by this utility should be considered estimates.

Potential sources of error include:

- All calculations are based on the entries in the event log. If the system time is altered significantly, this can have a dramatic affect on the calculations made. Additionally if the event logs have been cleared, or have filled, such that additional events cannot be written, this will also affect this tools ability to accurately estimate system availability.
- The system heartbeat is generally written every 5 minutes, so the amount of downtime calculated for abnormal outages is limited in accuracy to this window.
- Systems that are a member of a cluster are currently unsupported by Uptime.
- If Uptime detects that the target system may be a member of a cluster, Uptime will display a message stating that the results may be in error.

For further information about this utility, please see:

http://support.Microsoft.com/support and reference KB Article: Q232243

Note the following:

- Availability calculations require:
  - Windows NT 4.0 Service Pack 4 or higher, including Windows 2000.
  - The system heartbeat must be active.

  The system heartbeat is a date/time stamp that is written to the system registry at a fixed interval. This heartbeat is available in Service Pack 4 or higher. It is enabled by default on Windows NT Server. Since the heartbeat causes the registry to be written to the disk at regular intervals, it can interfere with systems running various forms of power management.

If the system heartbeat is disabled, or if you are not running Service Pack 4 or greater, Uptime may report that the event logs do not contain sufficient information to calculate system availability. This is because Uptime detects an abnormal shutdown (for instance a bluescreen or power failure) but cannot determine how long the system was down during this abnormal outage.

- No special privileges are required for basic operation although it is most accurate to run Uptime under an administrative account, since much more information is available to calculate system uptime and availability. For instance the time zone of the system is important to many of the calculations, but this information can only be reliably obtained by an administrator.

  Additionally, when calculating the Current System Uptime, this tool attempts to use the System Performance Counter for Uptime. However, if the user is not an administrator, this counter may be unavailable. In this case an estimate is made based on the last recorded boot noted in the event log.

- Application Failure event detection is dependent upon Dr Watson being enabled.
- Bluescreen detection is dependent upon the system being configured to write an event to the event log if the system stops unexpectedly.

  To enable bluescreen event logging for Windows NT 4.0 systems:

  - Go to the Windows Control Panel and double-click the System Icon.
  - Select the Startup/Shutdown tab.
  - Select the **Write an event to the system log** check box.

  To enable bluescreen event logging for Windows 2000 Systems:

  - Go to the Windows Control Panel and double-click the System Icon.
  - Select the Advanced tab.
  - From the Advanced property sheet select the Startup and Recovery button.
  - Select the **Write an event to the system log** check box.

To run the Uptime utility

1 If necessary, click the Diagnostics tab of the Management Console.

Click

2 Click the Uptime icon.

3 Click **Run**.

To change the Uptime utility settings

Based on the command syntax described below, enter the new command and arguments in the **Custom Arguments** text box and then click **Run**:

```
Uptime [server] [/s] [/a] [/d:mm/dd/yyyy | /p:n] [/heartbeat] [/?
| /help]
```

`server`	Name or IP address of remote server to process.
`/s`	Display key system events and statistics.
`/a`	Display application failure events (assumes /s).
`/d:`	Only calculate for events after mm/dd/yyyy.
`/p:`	Only calculate for events in the previous n days.
`/heartbeat`	Turn on/off the system's heartbeat
`/?`	Basic usage.
`/help`	Additional usage information.

Chapter 24

Entering and Activating Wave Licenses

CHAPTER CONTENTS

You configured your initial Wave licenses when you installed your Wave Server as described in Chapter 5 in the *Wave Server Installation Guide*. Follow the instructions in this chapter to add and activate additional licenses to add capacity or functionality to your Wave Server.

About the Wave Product Usage Improvement Plan

When you activate a license, you will be asked if you want to participate in the Product Usage Improvement Plan. Doing so will allow Vertical to gather installation, deployment, and usage information to better understand how customers configure and use , and assist in identifying and prioritizing areas for improvement. Participation in the plan is voluntary.

About Wave licenses

Wave licenses form the basis of your ability to install and use Wave. Keep your license information in a safe location and do not share it with others.

Wave licenses do the following:

- Control the ability to configure Wave system resources, for example VoIP resources, SIP phones, and so forth.
- Enable Wave workstation or add-on applications such as ViewPoint, Global Manager, Call Navigator, and so forth.

Important! New licenses are required in Wave ISM 2.0. Starting with Wave ISM 2.0, many of the core functionality licences from prior versions are no longer valid. In order for your Wave system to continue to function at its full capacity, you must install the new 2.0 licenses issued to you as part of your Software Subscription. Contact your Vertical support representative if you have not received your 2.0 licenses. For a description of the Wave licenses available starting in Wave ISM 2.0, see “Wave license requirements” on page 24-3.

Full vs. trial licenses

Wave licenses are available as full or trial licenses.

- A *full license* can be used for a period of time before it must be activated. If the grace period elapses and you do not activate the license, you will no longer be able to configure the type of system resource controlled by the license or use the add-on, as described in the table on page 24-4.
- A *trial license* lets you evaluate a feature or add-on for a period of time. Trial licenses cannot be activated—after the trial period expires, you must purchase a full license to continue using the feature or add-on.

Obtaining Wave licenses

Contact your Wave provider for the licenses required for your specific configuration. You may want to purchase additional licenses to allow for expected system growth so that you do not have to wait for a license the next time you want to expand your system.

Wave licenses are supplied by your Vertical provider in the following formats:

- **Wave license files**. License files can be imported directly onto the Wave Server. License files are named LICxxxxxxx.LIC, where x = the sales order number.
- **Acrobat file**. Each license file is accompanied by an Acrobat file that lists the included licenses. If the license file itself is lost or unreadable, you can enter the license keys in the associated Acrobat file manually.
- **Printed copy**. When you initially receive your Wave Server, a printed copy of your license information is included in the box.

Important! Before proceeding, ensure that you received the correct licenses by reviewing the Acrobat file that came with your license file or the printed copy that came with your Wave Server. If you have any questions, contact your Vertical provider before entering and activating the licenses.

Wave license requirements

Wave ISM supports scalability and edition-based licensing.

- **Scalability licenses** increase the maximum number of Wave users that can be added on a single system:
  - **Wave Professional Edition license**. Supports a maximum of 200 users/phones. You must add a Wave Professional Edition license to support this configuration.
  - **Wave Enterprise Edition license**. Supports a maximum of 500 users/phones. You must add a Wave Enterprise Edition license to support this configuration.
  - **Wave Standard Edition license**. Supports a maximum of 50 users/phones. There is no separate Standard Edition license—if you don't have a Wave Professional Edition license or a Wave Enterprise Edition license on your Wave Server, you have a Wave Standard Edition license.

- **Edition-based licenses** introduce dependencies between certain types of Wave licenses that are enforced when importing, adding, and deleting licenses.
    - **Wave SIP Trunk for Standard Edition license**. Requires a Wave Standard Edition license. See “Wave Standard Edition” above.
    - **Wave SIP Trunk for Professional Edition license**. Requires a Wave Professional Edition license.
    - **Wave SIP Trunk for Enterprise Edition license**. Requires a Wave Enterprise Edition license.
    - **WaveNet for Standard Edition license**. Requires a Wave Standard Edition license.
    - **WaveNet for Professional Edition license**. Requires a Wave Professional Edition license.
    - **WaveNet for Enterprise Edition license**. Requires a Wave Enterprise Edition license.

Wave ISM supports additional license types that enable specific functionality. If you do not have the correct number of Wave licenses entered, your ability to configure or use your Wave system will be affected in the following ways:

You need this license type:	
Wave ISM User	To add or modify a user via the User/Workgroup Configuration applet. This license also supports usage of the ViewPoint Softphone as a user’s secondary phone.
Wave IP Gateway	To configure VoIP resources via the Resource Management applet.
Wave IP User - Certified Third Party IP Phone	To configure a user to use a supported Aastra or Edge 1500-series SIP phone.
Wave IP User - Edge IP and ViewPoint Phone	To configure a user to use an Edge 5000-series SIP phone or the ViewPoint Softphone as his or her primary phone.
Wave IP User - Generic Third Party IP Phone	To configure a user to use a third-party SIP phone.
Wave SIP Trunk (Standard, Professional, or Enterprise Edition)	To configure a signaling control point (SCP) via the IP Telephony applet.
Wave ViewPoint	For each ViewPoint user, so that multiple Viewpoint users can concurrently access the Wave system.

You need this license type:	
Wave ViewPoint Mobile	For each ViewPoint Mobile user, so that multiple users can concurrently access the Wave system to make and take calls and access some ViewPoint features from supported mobile devices.
Wave ViewPoint Secondary Softphone	On a per-Wave Server basis, to provide support for the ViewPoint Softphone as users' secondary phone, if they are configured to do so.
Wave Contact Center Reporter	So that all ViewPoint users with the appropriate permissions can produce basic call and usage reports using the Contact Center Reporter. If you are also using the Wave Contact Center, a complete suite of queue reports is available.
Wave Contact Center Agent	For each user who is an agent in a Contact Center queue. Only one license is required for each agent, even if an agent is a member of multiple queues.
WaveNet (Standard, Professional, or Enterprise Edition)	On a per-Wave Server basis, so that a Wave Server can be a member of a WaveNet network.
Wave Call Classifier	On a per-Wave Server basis, so that the Wave Call Classifier add-on can be used to create rules to identify callers, intelligently route calls, and present Contact Center agents with scripts and related caller information before calls are answered.

Note: Outbound IVR applications and other Wave add-ons also require valid licenses. See the documentation for the specific application or add-on for licensing details.

Viewing the status of licenses on your system

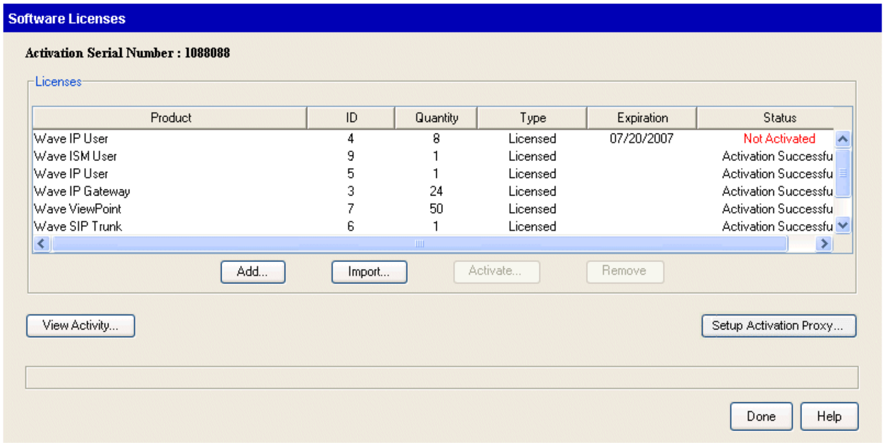
There are two ways to view the status of your Wave licenses:

- **Software Licenses applet**. See the instructions below.
- **License Status report**. You can run the License Status report using the Report Generator. This report reports on all Wave installed licenses by product name and version, and lists the license key, quantity, type, status, activation date (blank for a trial license), and expiration date (if applicable) for each license. See “Using the Report Generator” on page 31-25.

To view the status of licenses on your system at any time

1 On the Administration tab of the Global Administrator Management Console, select **Software Licenses**.

2 The Software Licenses applet starts and displays the status of all of the licenses on your system:



Software Licenses

Activation Serial Number : 1088088

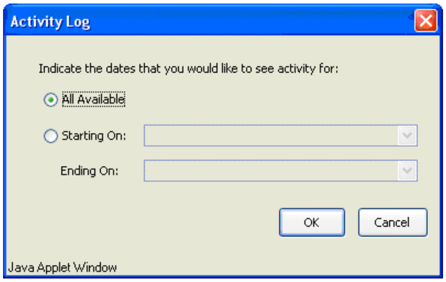
Licenses

Product	ID	Quantity	Type	Expiration	Status
Wave IP User	4	8	Licensed	07/20/2007	Not Activated
Wave ISM User	9	1	Licensed		Activation Successfu
Wave IP User	5	1	Licensed		Activation Successfu
Wave IP Gateway	3	24	Licensed		Activation Successfu
Wave ViewPoint	7	50	Licensed		Activation Successfu
Wave SIP Trunk	6	1	Licensed		Activation Successfu

Double-click on any license with a status of Activation Failed to view the reason for the failure.

3 To view license activity by date, click **View Activity**.

4 In the next screen, click **All Available** to display all licensing activities, or enter **Starting On** and **Ending On** dates to view licensing activities for a specific time period.



Activity Log

Indicate the dates that you would like to see activity for:

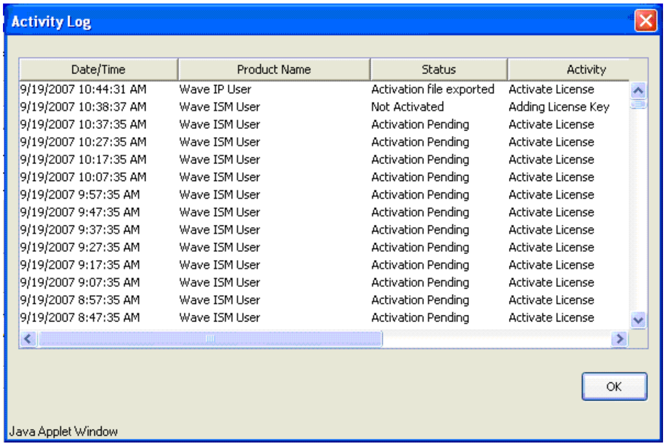
● All Available

○ Starting On:

Ending On:

5 Click **OK** to continue.

6 The Activity log opens showing the following information:



Activity Log

Date/Time	Product Name	Status	Activity
9/19/2007 10:44:31 AM	Wave IP User	Activation file exported	Activate License
9/19/2007 10:38:37 AM	Wave ISM User	Not Activated	Adding License Key
9/19/2007 10:37:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 10:27:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 10:17:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 10:07:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 9:57:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 9:47:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 9:37:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 9:27:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 9:17:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 9:07:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 8:57:35 AM	Wave ISM User	Activation Pending	Activate License
9/19/2007 8:47:35 AM	Wave ISM User	Activation Pending	Activate License

7 Click **OK** to close the Activity Log.

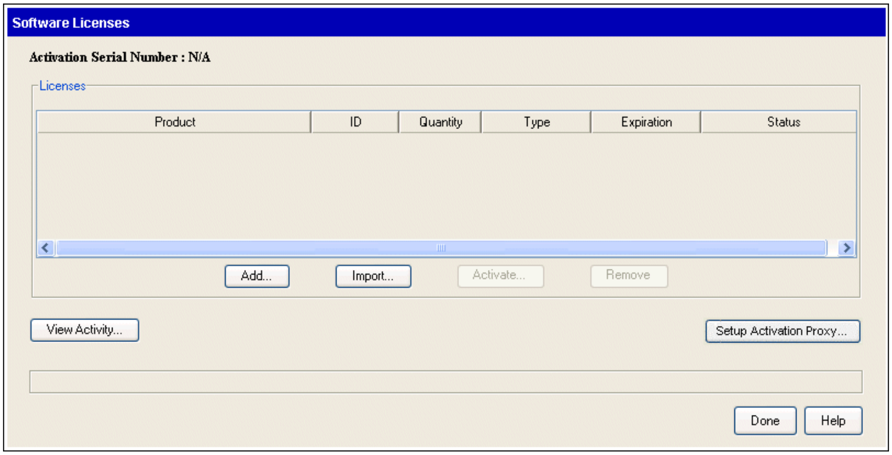
Entering Wave licenses

You can add Wave licenses to the Wave Server in either of the following ways:

- Import a license file, as described in the next section.
- Enter the license key for each license, as described on page 24-10.

Entering Wave licenses by importing a license file

1 On the Administration tab of the Global Administrator Management Console, select **Software Licenses**. The Software Licenses applet starts and displays any licenses that have already been entered:

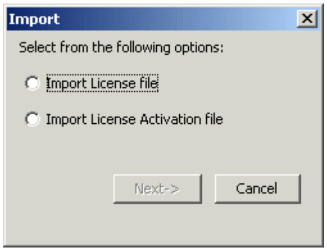


Software Licenses

Activation Serial Number : N/A

Product	ID	Quantity	Type	Expiration	Status

2 Click **Import**. When the Import dialog opens, click **Import License file** and then click **Next**.



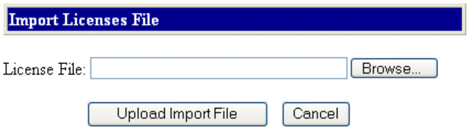
Import

Select from the following options:

○ Import License file

○ Import License Activation file

3 In the Import Licenses File dialog, click **Browse** to go to the license text file that you want to import.


Import Licenses File

License File:

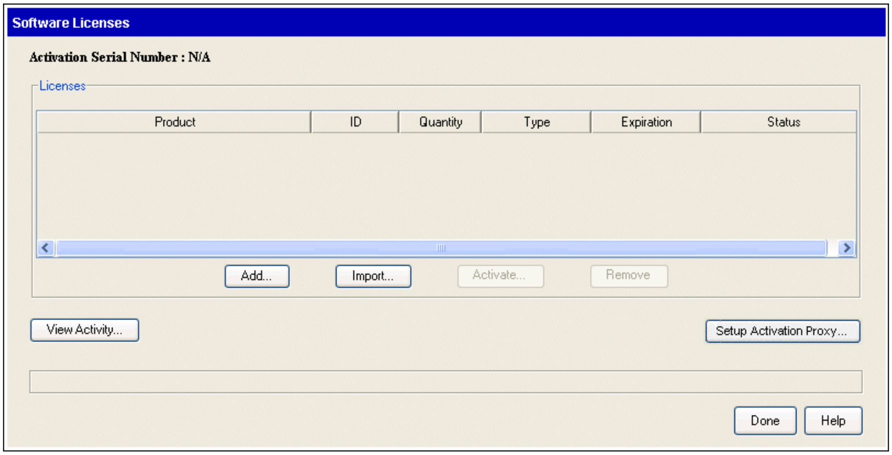
4 In the Choose File dialog, select the license file and then click **Open** to return to the Import Licenses File dialog.

5 Click **Upload Import File**. A list of all of the licenses in the file is displayed. Scroll to the bottom of the list and click **Done**.

6 After the import finishes, the Import Licenses File dialog opens again. Click **Cancel** to return to the Software Licenses applet. Go to “Activating Wave licenses” on page 24-11.

Entering Wave license keys for each license

1 On the Administration tab of the Global Administrator Management Console, select **Software Licenses**. The Software Licenses applet starts and displays any licenses that have already been entered:

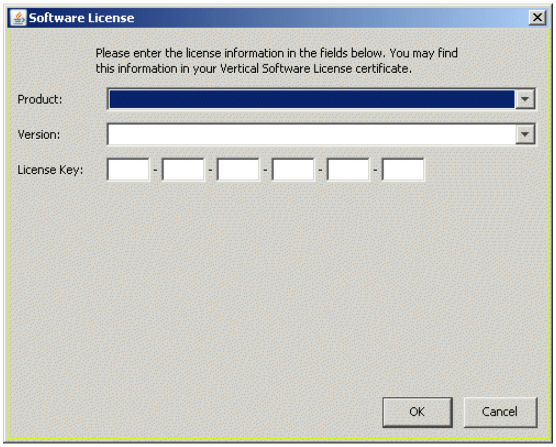


Software Licenses

Activation Serial Number : N/A

Product	ID	Quantity	Type	Expiration	Status

2 Click **Add**. The Software License dialog opens:



Software License

Please enter the license information in the fields below. You may find this information in your Vertical Software License certificate.

Product:

Version:

License Key: - - - - -

3 Enter the following information:

- Select the **Product** for which you want to enter licenses from the drop-down list.
- Select the **Version** number for that product.
- Enter the full 24-character **License Key**.

4 Click **OK**. The license you added is now displayed.

5 To add additional licenses, repeat steps 2-4. When you are done, go to the next section to activate the new licenses.

Activating Wave licenses

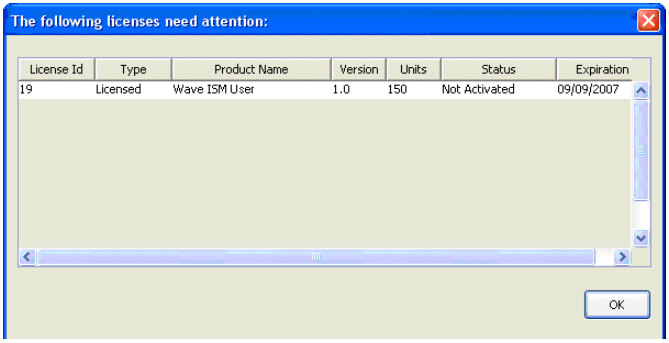
You activate your Wave licenses to enable full functionality on your Wave system. Once you have entered your licenses, you are ready to activate them.

Before your licenses are activated

You can use non-trial Wave licenses for a period of time without activating them (the specific period of time can vary by license type.) The grace period starts on the day that you enter the license via the Software Licenses applet. You can activate your licenses at any time during the grace period or after the grace period elapses.

Until you activate your licenses, the following will occur:

- Every time you launch the Global Administrator Management Console, you will be reminded that licenses need to be activated. The dates when license grace periods are due to elapse are displayed in the Expiration column



The following licenses need attention:

License Id	Type	Product Name	Version	Units	Status	Expiration
19	Licensed	Wave ISM User	1.0	150	Not Activated	09/09/2007

- If the grace period expires before a license is activated, whenever any user accesses their voice messages, the user hears a message stating that there is an expired license on the system and to contact the system administrator.

Activating your licenses eliminates these behaviors, and prevents any interruption to your system's operation if the grace period expires.

Important! Whenever you activate licenses, be sure to back up your Wave system according to the instructions in "Backing up your Wave system configuration" on page 15-2Backing up your Wave system configuration so that you do not have to repeat the activation process if you ever need to restore your system.

The activation process

Activation consists of the following steps:

1 You submit your license information to Vertical using either of the methods described below.

2 Vertical verifies the information. When you activate your licenses, the registration information that you submit to Vertical is verified and saved for future troubleshooting purposes. You have the opportunity to review the details of Vertical's privacy statement during the activation process detailed later in this chapter.

3 Activated licenses are returned to you and applied to your system.

One-click vs. offline activation

There are two ways to activate your Wave licenses:

- **One-click activation.** Use this method if the Wave Server has an Internet connection that allows the use of the HTTPS protocol, and you have a valid DNS server. (See Chapter 6 in the *Wave Server Installation Guide* for more about configuring the Wave Server for one-click activation.) If you encounter problems with one-click activation, you can try offline activation, or contact your Vertical provider.

  Note that if your Wave Server does not meet these requirements, you can still use one-click activation if you set up a license activation proxy server. See page 24-20 for more information.

  One-click activation steps start on page 24-14.

- **Offline activation.** Use this method if the Wave Server does not have Internet access or does not allow the use of the HTTPS protocol. With offline activation, you generate an Offline Activation Request and submit it to the Vertical Activation Web site from another PC. An Activation File is returned to you that you then manually activate on the Wave Server.

  Offline activation steps start on page 24-16.

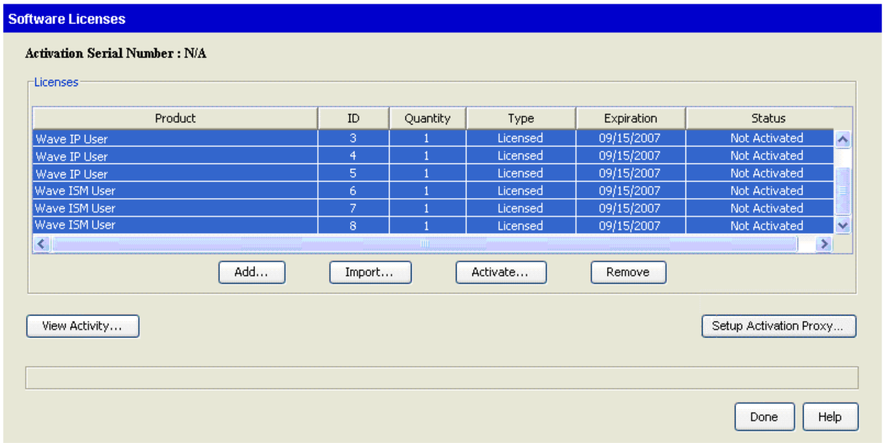
Activation results

If activation is successful, activated licenses are returned and automatically added to your system. You are returned to the screen that displays all of your licenses. Note that the Status column will not update until you exit and restart the Software Licenses applet.

If activation is not successful, the reason is displayed. The most common status resulting from an unsuccessful one-click activation, “Activation Pending”, indicates a bad Internet connection, or that the Vertical Activation Server is down; the system will retry activation automatically. If you continue to experience problems, try offline activation, or contact your Vertical representative.

Activating your Wave licenses using one-click activation

1 In the Software Licenses applet, click one license to activate it or Ctrl-click to select multiple licenses.



Software Licenses

Activation Serial Number : N/A

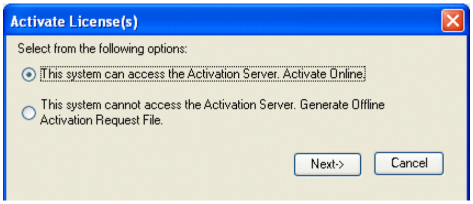
Licenses

Product	ID	Quantity	Type	Expiration	Status
Wave IP User	3	1	Licensed	09/15/2007	Not Activated
Wave IP User	4	1	Licensed	09/15/2007	Not Activated
Wave IP User	5	1	Licensed	09/15/2007	Not Activated
Wave ISM User	6	1	Licensed	09/15/2007	Not Activated
Wave ISM User	7	1	Licensed	09/15/2007	Not Activated
Wave ISM User	8	1	Licensed	09/15/2007	Not Activated

Note: Only those licenses that are in the statuses of Not Activated, Activation Pending, and Activation Failed can be selected for Activation. Double-click on any license with a status of Activation Failed to view the reason for the failure.

2 Click **Activate**. To continue, accept the Vertical Communications Privacy Statement and then click **OK**.

3 The Activate Licenses dialog opens. Select **This system can access the Activation Server. Activate Online**, and then click **Next**.



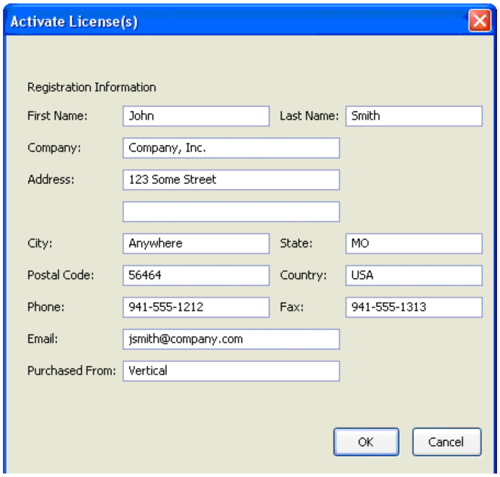
Activate License(s)

Select from the following options:

● This system can access the Activation Server. Activate Online

○ This system cannot access the Activation Server. Generate Offline Activation Request File.

4 In the next screen, enter registration information about your organization. You must enter at least **First Name** and **Last Name** to enable the **OK** button in order to continue.



Registration Information

First Name:	John	Last Name:	Smith
Company:	Company, Inc.		
Address:	123 Some Street		
City:	Anywhere	State:	MO
Postal Code:	56464	Country:	USA
Phone:	941-555-1212	Fax:	941-555-1313
Email:	jsmith@company.com		
Purchased From:	Vertical		

5 Click **OK** to submit the selected licenses for activation. During activation, the Activate Licenses dialog (with the registration information cleared) is displayed.

6 Return to the Software Licenses dialog. (The license Status column will not update until you exit and restart the Software Licenses applet.)

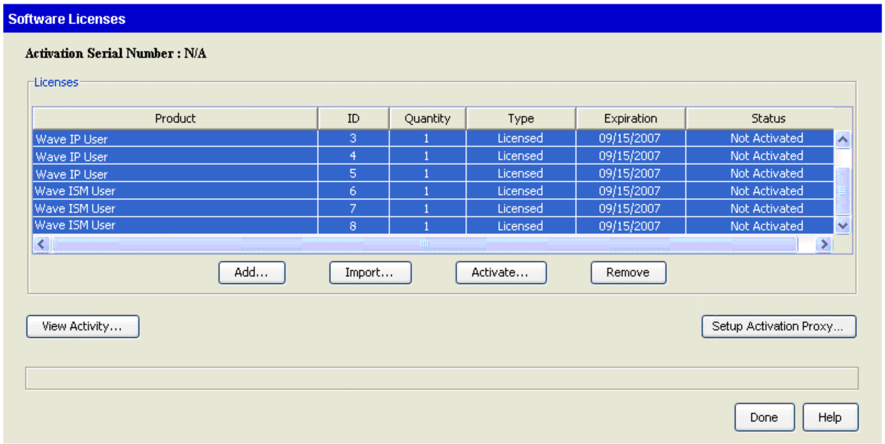
7 Click **Done** to return to the Global Administrator Management Console.

Activating your licenses using offline activation

Offline license activation occurs in 2 stages:

- You generate an Activation Request file and submit it to the Vertical Activation Web site.
- You receive an Activation file in response, and activate it.

1 In the Software Licenses applet, click one license to activate it or Ctrl-click to select multiple licenses.



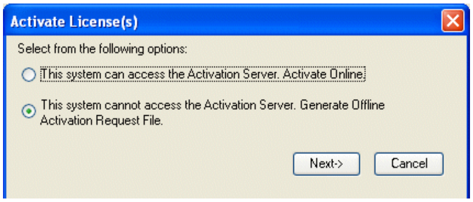
Activation Serial Number : N/A

Product	ID	Quantity	Type	Expiration	Status
Wave IP User	3	1	Licensed	09/15/2007	Not Activated
Wave IP User	4	1	Licensed	09/15/2007	Not Activated
Wave IP User	5	1	Licensed	09/15/2007	Not Activated
Wave ISM User	6	1	Licensed	09/15/2007	Not Activated
Wave ISM User	7	1	Licensed	09/15/2007	Not Activated
Wave ISM User	8	1	Licensed	09/15/2007	Not Activated

Note: Only those licenses that are in the statuses of Not Activated, Activation Pending, and Activation Failed can be selected for Activation. Double-click on any license with a status of Activation Failed to view the reason for the failure.

2 Click **Activate**. To continue, accept the Vertical Communications Privacy Statement and then **OK**.

3 The Activate Licenses dialog opens. Select **This system cannot access the Activation Server. Generate Offline Activation Request File**, and then click **Next**.

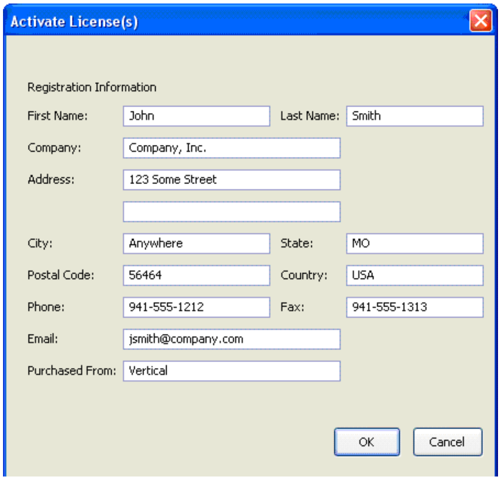


Select from the following options:

○ This system can access the Activation Server. Activate Online

● This system cannot access the Activation Server. Generate Offline Activation Request File.

4 In the next screen, enter registration information about your organization. You must enter at least **First Name** and **Last Name** to enable the **OK** button in order to continue



Registration Information

First Name:	John	Last Name:	Smith
Company:	Company, Inc.		
Address:	123 Some Street		
City:	Anywhere	State:	MO
Postal Code:	56464	Country:	USA
Phone:	941-555-1212	Fax:	941-555-1313
Email:	jsmith@company.com		
Purchased From:	Vertical		

5 A file save dialog opens. Choose to save the file, then in the Save As dialog name the file and specify the save location. Make a note of the file’s name (the default file name is ActivationRequestFileName.lic) and location,.

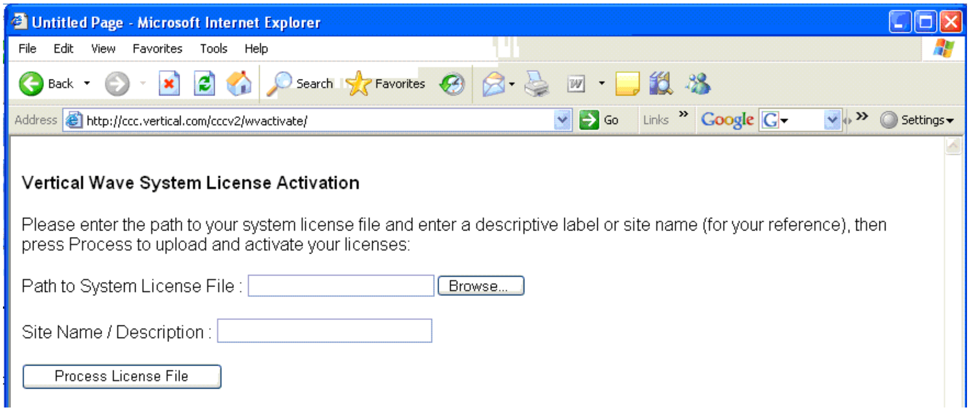
Go to step 6.

> **Important!** If you fail to see a file save dialog but see instead a screen of encrypted characters, you must reconfigure the Wave Server to save rather than open LIC files. To do so, perform the steps on page 24-20, and then begin the offline license activation process again, starting at step 1 on page 24-16.

6 Start another instance of Internet Explorer, and then enter and go to the following URL address:

https://activate.vertical.com

7 Click **Yes** if you are asked whether to trust the site. You are taken to the Vertical Wave System License Activation Web page.


Untitled Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://ccc.vertical.com/cccv2/wvactivate/
Go
Links
Google
Settings

Vertical Wave System License Activation

Please enter the path to your system license file and enter a descriptive label or site name (for your reference), then press Process to upload and activate your licenses:

Path to System License File : Browse...

Site Name / Description :

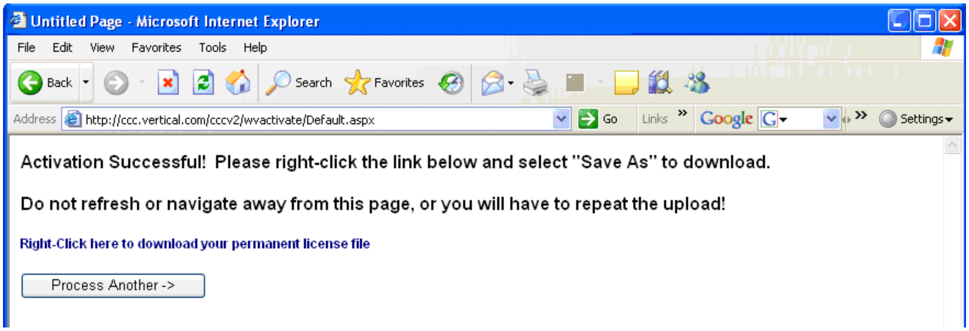
Process License File

8 Enter the following information:

- **Path to System License File**. Type the path and file name of the LIC file that you saved earlier, or click **Browse** to specify it.
- **Site Name / Description**. For your own reference, enter identifying information about the license file, for example, “CambridgeLicenses”.

9 Click **Process License File**. Activation may take a few seconds to 2-3 minutes.

10 If activation is successful, you will see the following web page. Click **Right-click here to download your permanent license file**.


Untitled Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://ccc.vertical.com/cccv2/wvactivate/Default.aspx
Go
Links
Google
Settings

Activation Successful! Please right-click the link below and select "Save As" to download.

Do not refresh or navigate away from this page, or you will have to repeat the upload!

Right-Click here to download your permanent license file

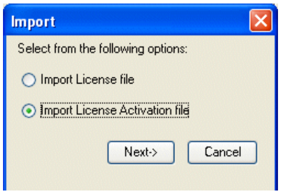
Process Another ->

If activation was unsuccessful, the error or errors are displayed on-screen.

11 A file save dialog opens. Choose to save the file, then in the Save As dialog, name the file and specify the save location. Make a note of the file's name and location.

12 Click **Process Another ->** to activate another Activation Request File, or return to the Software Licenses applet if you are done.

13 Click **Import**. When the Import dialog opens, click **Import License Activation file** and then click **Next**.



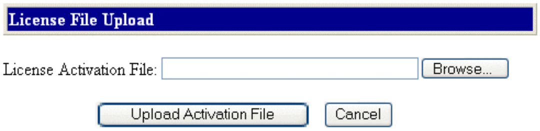
Import

Select from the following options:

○ Import License file

● Import License Activation file

14 In the License File Upload dialog, click **Browse** to go to the Activation Request File that you downloaded and saved from the Vertical License Activation web page.



License File Upload

License Activation File:

15 In the Choose File dialog, select the Activation Request File and then click **Open** to return to the License File Upload dialog.

16 Click **Upload Activation File**.

17 A list of all of the licenses in the file is displayed. Scroll to the bottom of the list and click **Done**.

18 After the upload finishes, the License File Upload dialog opens again. Click **Cancel** to return to the Software Licenses applet. (The license Status column will not update until you exit and restart the Software Licenses applet.)

19 Click **Done** to return to the Global Administrator Management Console.

Configuring the Wave Server to save rather than open License files

Perform the steps in this section if you are directed to do so in step 5 in “Activating your licenses using offline activation” on page 24-16.

1. In Windows Explorer (not Internet Explorer), choose **Tools > Folder Options** to open the Folder Options dialog.
2. On the File Types tab, select **LIC** in the **Extensions** column, and then go to step 8.

   If there is no LIC entry in the **Extensions** column, you must create one. To do so, click **New**.
3. In the Create New Extension dialog, enter LIC in the **File Extension** field, and then click **Advanced>>**.
4. Select **License** from the **Associated File Type** drop-down list. Click **OK** to return to the Folder Options dialog.
5. Click **Advanced** to open the Edit File Type dialog.
6. Check **Confirm open after download**, and then click **New** to open the New Action dialog.
7. In the **Application used to perform action** field, enter the following:

   C:\WINDOWS\system32\NOTEPAD.EXE %1

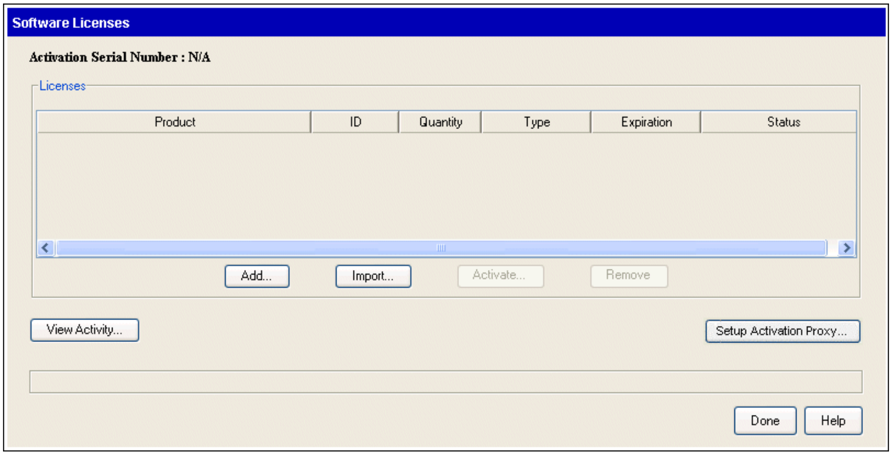
   You can specify a different text editor if you prefer.
8. Click **OK** to close all dialogs.
9. Begin the offline license activation process again, starting at step 1 on page 24-16.

Setting up a proxy server for license activation

You can set up a proxy server on another PC on your network to act as an interface between your Wave Server and the Vertical License Activation Web page. The proxy server PC must have Internet access and allow the use of the HTTPS protocol, and you must have a valid DNS server on your network.

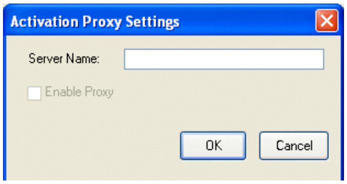
- A proxy server is useful if the Wave Server does not have Internet access or does not allow the use of the HTTPS protocol, and you want to be able to use one-click license activation (instead of offline activation).
- You MUST use a proxy server for license activation if a Wave license file consists of a single license key for unlimited site usage.

1 In the Software Licenses applet, click **Setup Activation Proxy**.



Activation Serial Number : N/A

2 In the Activation Proxy Settings dialog, enter the following information:



- **Server Name**: Name of the PC on your network to be used as the license activation proxy server. **Server Name** can consist of a maximum or 20 alphabetic and numeric characters including dashes, periods, underlines, and parenthesis, but i cannot contain blanks.
- **Enable Proxy**: Select this checkbox to enable the license activation proxy server. This checkbox is disabled until you enter a valid **Server Name**.

3 Click **OK**.

Chapter 25

Connecting Wave Servers via WaveNet

CHAPTER CONTENTS

About WaveNet

With WaveNet, you can connect multiple Wave Servers so that selected users can be shared between Servers and can be seen and used as if they are on a single large system.

The following terminology is used throughout this chapter:

- A *node* is any Wave Server connected via WaveNet.
  - A *local node* is the node in a WaveNet network that you are connected to, either via a phone, ViewPoint, or the Wave Global Administrator Management Console. The local node is “local” from your point of view.
  - A *remote node* is another node in a WaveNet network to which you are not connected. A remote node is “remote” from the point of view of the local node.
  - A *home node* is the Wave Server where a local user was originally created.
  - A *publishing node* is the Wave Server from which information about local users is sent to one or more remote nodes.
  - A *subscribing node* is the Wave Server that receives information about users on other nodes.

- A *user* is a Wave user on one of the Wave Servers in the WaveNet network:
  - A *local user* is a Wave user whose “home” is the local Wave Server.
  - A *Gateway user* is a Wave user whose “home” is another node in the WaveNet network, from the point of view of the local node. A Gateway user acts as a place holder, and is really an off-premise extension that points to the real user who is “local” on another Wave Server.

This section discusses the following topics:

- About users in a WaveNet network. See page 25-2.
- About publication and subscription. See page 25-3.
- About automatic trunking and routing configuration. See page 25-3.
- About performing a system backup or restore on a WaveNet node. See page 25-4.
- Limitations in this version. See page 25-5.

About users in a WaveNet network

By replicating local users on one Wave Server to other nodes in the WaveNet network, it appears as if the system administrator has added each user locally.

The following user information is replicated from a Gateway user’s home node to subscribing remote nodes:

- **User information**. Name, extension, greetings, voice title, and so forth.
- **Personal status**. Available, Do Not Disturb, In A Meeting, Out Of The Office, or On Vacation, or any other personal statuses that have been defined.
- **Availability**. On-hook, off-hook, ringing.
- **Contacts**. A Gateway user’s contacts that have PIN numbers are replicated to subscribing nodes. This allows a call to be identified as from that contact no matter which node in the WaveNet network handled the call. A voice message left by that contact at a remote node will also be identified as from the contact when it is delivered to the user’s home node voice mailbox. (Contacts that do not have PIN numbers, and any other contact information—for example, phone numbers—are not currently replicated.)

The following user information is transferred from remote nodes to a GateWay user's home node:

- **Voice Mail**. Messages recorded on remote nodes are sent to the GateWay user's home node voice mailbox.

About publication and subscription

The process of replicating users is called “publishing”. You publish one or more users *from* the Wave Server where those users live *to* other nodes. Publication pushes the user information listed above, as well as any subsequent updates to that information for those users, to the other nodes that you specify.

On each other Wave Server, a Gateway user is created for each published user. Those users are said to be “subscribed”.

Important! You do not need to publish all of the users on a Wave Server. Since initial publication and subsequent updates can generate a substantial amount of network traffic, you should publish only those users or extensions that need to be directly dialed from other nodes.

Publication steps are described in “Publishing local users on remote nodes” on page 25-20.

What happens when users are deleted from the network?

If you delete a published user from a node, that user’s off-premise extension representation is deleted from the subscribing node. When the last user published from a node is deleted, the SCP, routing table, and routing rule used to route calls back to that node are automatically deleted from the subscribing node.

About automatic trunking and routing configuration

When you publish the first local user to another node, WaveNet automatically sets up the following on the subscribing node:

- One *SIP signaling control point (SCP)*, used to route calls back to the Gateway user’s home node. (SIP signaling control points determine how IP calls are handled to and from specific IP addresses.)
- *One routing table* with *one SIP trunk routing rule* per table.

All Gateway users published from that same node use the same SCP and routing table on the subscribing node.

In addition, the following is set up for each Gateway user on the subscribing node:

- An *off-premise extension* representation. Either as a single off-premise extension, or as part of a range of an extension range.

About performing a system backup or restore on a WaveNet node

When you perform a system backup on a Wave Server that is also a node in a WaveNet network, the WaveNet databases are included in the backup. See “Special Backup/Restore considerations on a WaveNet node” on page 15-5 for important information.

What information is transmitted when a call is transferred from one WaveNet node to another?

WaveNet calls are transmitted over SIP trunks from one node to another. All calls are normal SIP calls. The following information is transmitted when a WaveNet call is transferred from one node to another:

- **CallerID**.
  - For a supervised transfer, this will be the *transferring station*’s Caller ID.
  - For a blind transfer, this will be *original* Caller ID associated with the call.
- **Destination extension**, in the DID field. The original inbound call DID information is overwritten when the call is redirected via WaveNet.
- **VID**. This value uniquely identifies the call when it is transferred across WaveNet nodes, and remains the same throughout the Wave network for the life of the call.

Important! No other information is transmitted with a call via WaveNet. Call notes, custom data, account codes, and other rich data fields are not transmitted between WaveNet nodes.

Limitations in this version

Note the following limitations in this version:

- SIP trunking is the only currently supported trunk type.
- Only one SIP SCP can be configured on a Wave Server that points to the same endpoint and port. See “SIP signaling control point (SCP) issues” on page 25-6 for important information regarding this restriction.
- A maximum of 1500 Gateway user subscriptions can be created per Wave Server.
- A maximum of 100 Wave Servers can be added to a WaveNet network.
- Network Address Translation (NAT) is not supported for use with WaveNet.

Planning for WaveNet

Connecting multiple Wave Servers together via WaveNet requires thorough planning in order to have a smoothly running WaveNet network. This includes configuring the TCP/IP connectivity between network nodes, designing a global extension plan for users across all network nodes, configuring trunking and dialing access plans between nodes—all have to work together to make a WaveNet network easy to use.

This section discusses the following WaveNet planning topics:

- TCP/IP connectivity between proposed nodes. See page 25-6.
- Trunking considerations. See page 25-6.
- Dial plan considerations. See page 25-7.
- Virus-scanning issues. See page 25-11.

TCP/IP connectivity between proposed nodes

- **Use static IP addresses**. WaveNet requires that the IP address of each WaveNet node is a static IP address. Dynamic (DHCP) addresses are not supported.
- **Verify connectivity between nodes**. Before WaveNet can be expected to communicate between nodes, it is essential to first establish that the network connections from each node to all other nodes are functioning properly.

  Ping can be used in both directions between proposed WaveNet nodes to verify basic network connectivity between the nodes, but it will not determine if the MSMQ port and/or SIP ports are usable between the nodes (see the next bullet.)
- **Configure required ports between nodes**. The following ports are required to support communication between WaveNet nodes:
  - **Microsoft Message Queue (MSMQ)**. TCP Port 1801.
  - **SIP ports**. For details on how to set up SIP telephony on a Wave Server, see Chapter 6.

Trunking considerations

Important! In the current version, only SIP trunking is supported.

This section describes the following:

- SIP signaling control point (SCP) issues. See page 25-6.

SIP signaling control point (SCP) issues

When you publish a user to one or more remote nodes, WaveNet automatically creates one SIP SCP on each remote node (as described in “About automatic trunking and routing configuration” on page 25-3).

Important! The current version does not support two SCPs that point to the same endpoint *and* port. (An “endpoint” is a Wave Server, a WaveNet node, or another system.) The IP Telephony applet in the Global Administrator Management Console will not allow you to create such duplicates, and WaveNet will not automatically create any duplicate SCPs.

You may have pre-existing non-WaveNet SCPs to support off-premise extensions, external dialing, private networking, and so forth. If any of these pre-existing SCPs point to any of the Wave Servers that you plan to add as nodes in the WaveNet network, and they are configured to use the same port as the default SIP listener port on those nodes, you must manually delete the pre-existing SCPs or move them to a different port, to allow WaveNet to create the SCPs that it needs to point to these nodes in order to deliver calls to published Gateway users.

After the WaveNet SCPs have been automatically created, you can do either of the following to restore off-premise extensions, external dialing, or private networking previously associated with any SCPs that were deleted:

- Create new SCPs with the same endpoint address, but with different ports.
- Share the WaveNet SCPs for those other purposes. Note that while the WaveNet SCPs can be used this way, they cannot be edited in any way. This method is not recommended, because future changes might create a confusing situation involving the WaveNet created SCPs.

Example: Centralized Trunking SCPs

If SIP trunking between WaveNet nodes is required to deliver calls to a node with centralized trunking, then define a separate reciprocal pair of SCPs using a different port. Each node should have a new non-WaveNet SCP defined with the endpoint address of the reciprocal node, but use a different port (examples: 5061, 5070, etc.) Route calls for the centralized trunks (or any other non-WaveNet purposes) over this non-WaveNet pair of SCPs.

Dial plan considerations

Defining a comprehensive dialing plan is critical to the success of your WaveNet network, as well as for continued or future support of non-WaveNet dialing functionality.

This section describes the following:

- Local and network extension plan issues. See page 25-8.
- First Digit Table issues. See page 25-8.
- External dialing issues. See page 25-10.
- Non-WaveNet off-premise extension issues. See page 25-10.
- Private networking issues. See page 25-11.

Local and network extension plan issues

No two extensions, whether local user extensions or Gateway user extensions, can be exactly the same if they are shared to the same node. Careful planning can avoid future “collisions” of duplicate extension numbers when users are published to other nodes that will then need to be resolved one by one.

- **Number of extensions required**. How many local user extensions do you need? How many Gateway user extensions do you need?
- **Extension length**. Extension length determines the maximum number of extensions possible locally, and across the network. Any WaveNet location-based prefixes, for example “Store Number” should be taken into consideration when deciding on extension length.
    - **Same length**. Making both local user extensions and Gateway user extensions the same length is easiest to explain to users, because there is no difference between dialing a local user vs. a published Gateway user. However, you must ensure that there are no duplicated extensions anywhere.
    - **Different lengths**. You may need to implement extensions of different lengths if you are using a prefix system, since the prefix will be prepended onto the local extensions before they are published. Users may find it confusing to have to dial extensions of different lengths depending on whether they are dialing a local user or a published Gateway user. However, there is no risk of duplication between local user extensions and Gateway user extensions.

First Digit Table issues

You need to carefully coordinate the First Digit Tables of all the nodes in the network. In order for any Wave extension (local user extension or Gateway user extension) to be dialed successfully:

- The first digit of that extension must match an entry in the First Digit Table.
- That First Digit must be configured as **Extension**.
- The extension length for that First Digit must match the actual length of the extension.

For example, for extension 3005 to be dialed successfully, the following entry must be defined in the First Digit Table:

Digit (Type) = 3 (Extension)

Extension Length = 4

When you publish one or more local users to a remote note, the extensions of those users are compared against the First Digit Table on the subscribing node. WaveNet will not accept a publication request when the First Digit Table on the subscribing node cannot meet the requirements listed above.

The possible scenarios are:

- **First digit not yet configured**. If the first digit of a user’s extension is currently not in use (set to **Not Configured**) in the First Digit Table, WaveNet automatically updates the First Digit Table and sets the digit type to **Extension** and extension length to the actual length of the user’s extension. The publication request for this user is accepted, and the corresponding Gateway user is created on the subscribing node.
- **First Digit configured as Extension with correct length.** If the first digit of a user’s extension is currently in use and set to **Extension** in the First Digit Table, the length of the user’s extension is compared to the **Extension Length** for that First Digit.
    - If the lengths match, the publication request for this user is accepted, and the corresponding Gateway user is created on the subscribing node.
    - If the lengths do not match, the publication request is rejected with the error “User Exception - First Digit Length”.
- **First Digit configured as Attendant or External**. If the first digit of a user’s extension is currently defined and set to **Attendant** or **External** in the First Digit Table, the publication request is rejected with the error “User Exception - Already in Use”.

Important! If the publication request is accepted (either because the First Digit was previously **Not Configured**, or was configured as **Extension** with the correct length), WaveNet flags that First Digit as “Protected”, to prevent any inadvertent changes that would prevent Gateway users whose extension matches that first digit from being dialed.

External dialing issues

A First Digit Table entry set to **External** defines 1-2 digit access code used to make an external call.

Note the following:

- Digit combinations used for external dialing cannot be duplicated by any Gateway user extensions used with WaveNet.
- Any SCP currently used for external dialing that points to a Wave Server that is also a WaveNet node must be manually deleted or moved to a different port before publishing any users to that Server.

Non-WaveNet off-premise extension issues

Before deploying WaveNet, you may have already configured off-premise extensions that you want to continue using, or you may want to create them in the future for purposes unrelated to WaveNet.

As long as there are no duplicate extension numbers, non-WaveNet off-premise extensions are supported on the same Wave Server as the ones that WaveNet creates automatically for Gateway users published from other nodes.

- If any non-WaveNet off-premise extensions already exist on a Wave Server with the same extensions as users that will be published from any other nodes in the WaveNet network, those off-premise extensions must first be deleted or assigned a different extension number before publication will be successful.
- If you want to create new non-WaveNet off-premise extensions on a Wave Server that is a node in a WaveNet network, you must either:
  - Assign extension numbers to the new off-premise extensions that do not duplicate any existing subscribed Gateway users’ extensions.
  - Delete the subscribed Gateway users before creating the non-WaveNet off-premise extensions using those extension numbers.

Also, any SCP currently used for off-premise extensions that points to a Wave Server that is also a WaveNet node must be manually deleted before publishing any users to the Server.

Private networking issues

To dial an extension via a private network, a user must dial the following:

- **External access code** of 2 or more digits to access the private network.
- **Location code** of 2-6 digits to identify the Wave Server of the extension being dialed.
- **Called party's extension**.

A WaveNet network and a private network can coexist, however note the following:

- External access code + location code + called party extension digit combinations used for private networking cannot be duplicated by any Gateway user extensions used with WaveNet.
- Any SCP currently used for private networking that points to a Wave Server that is also a WaveNet node must be manually deleted before publishing any users to the Server.

For details on setting up a private network, see "Configuring private networking" on page 9-29.

Virus-scanning issues

It is important to achieve a balance between ensuring a secure and virus-free environment while also not interfering with the reliability and performance on each Wave Server. One contributing cause of application and service outages or system performance issues may be not configuring adequate exclusions if you use virus-scanning software.

Current best practice is to exclude the following Microsoft Message Queue (MSMQ) folders from virus scanning:

```
%SystemRoot%\system32\MSMQ
%SystemRoot%\system32\MSMQ\storage
```

Important! Applying this exclusion is at your discretion. Applying any exclusion to your virus-scanning configuration may make your Wave Server or your network more vulnerable to attack by malicious users or by malicious software such as viruses. Before making any changes, it is recommended that the risks associated with configuring virus-scanning exclusions be evaluated thoroughly. Depending on the specifics of your environment, additional settings may be required to prevent reliability and/or performance issues.

Installing WaveNet

Once your Wave Server meets the requirements listed below, the WaveNet applet in the Global Administrator Management Console will be operational—no additional installation steps are required.

Perform the following steps on each Wave Server that will be added as a node in the WaveNet network.

1. Make sure that each Wave Server in the WaveNet network meets the following requirements:
   - Install or upgrade the Wave Server to the required versions. For the latest information, contact your Vertical provider.
   - Purchase, enter, and activate required one WaveNet license per Wave Server. For more about Wave licenses, see Chapter 24.
2. Obtain the following logon accounts:
   - A logon account with Enterprise rights on your Wave Server.
   - Logon accounts for other nodes:
     - **If you are adding your Wave Server to an existing WaveNet network**. Obtain an Enterprise logon account from any other node in the network.
     - **If you are building a new WaveNet network**. Obtain an Enterprise logon account from each other Wave Server that you will add as a node.

   Note: Providing valid credentials when adding a Wave Server helps ensure that only approved nodes are added to the network.
3. Manually eliminate off-premise extension conflicts:
   - **Local off-premise extension conflicts**. Delete any off-premise extensions configured on your local Wave Server that would be duplicated by Gateway user extensions to be published from remote nodes to your local Wave Server.
   - **Remote off-premise extension conflicts**. Delete any off-premise extensions configured on remote nodes that would be duplicated by Gateway user extensions that you plan to publish to those remote nodes after you add your local Wave Server to the WaveNet network.

   See “Non-WaveNet off-premise extension issues” on page 25-10 for more information.

4 Manually eliminate First Digit Table conflicts.

- **Local First Digit Table conflicts**:
    - Any local First Digits that match the first digit of any Gateway user extensions that will be published on the local Wave Server, must either be **Unassigned**, or set to **Extension**, with the correct length for those Gateway user extensions.
    - Any local First Digits set to **External** that utilize an SCP that points to a Wave Server that is also a WaveNet node must be manually deleted before publishing any users to the Server. Once the WaveNet SCP has been automatically created, the First Digit can be re-added sharing the WaveNet SCP to restore external dialing.
- **Remote First Digit Table conflicts**:
    - Any remote node First Digits that match the first digit of any Gateway user extensions that will be published on the those remote Wave Servers, must either be **Unassigned**, or set to **Extension** with the correct length for those Gateway user extensions.
    - Any remote node First Digits set to **External** that utilize an SCP that points to a Wave Server that is also a WaveNet node must be manually deleted before publishing any users to the Server. Once the WaveNet SCP has been automatically created, the First Digit can be re-added sharing the WaveNet SCP to restore external dialing.

See “First Digit Table issues” on page 25-8 for more information.

5 Manually eliminate SCP conflicts to prevent possible inbound SIP call routing problems.

- **Local SCP conflicts**. For any remaining SCPs on the local node that point to other Wave Servers that are also WaveNet nodes (for example SCPs used for off-premise extensions, private networking, and so forth), manually delete those SCPs or move them to a different port than the default SIP listener port on those nodes.
- **Remote SCP conflicts**. For any remaining SCPs on any remote node that point to other Wave Servers that are also WaveNet nodes (for example SCPs used for off-premise extensions, private networking, and so forth), manually delete those SCPs or move them to a different port than the default SIP listener port on those nodes.

See “SIP signaling control points (SCPs) issues” in “Trunking considerations” on page 25-6 for more information.

6 In the General Settings applet, on the PBX (Advanced) tab select the **Allow Trunk-To-Trunk Connections** checkbox. (This setting allows inbound calls on the Wave Server to be routed to Gateway users on other WaveNet nodes.)

7 If you are using anti-virus software, configure that software to exclude the following Microsoft Message Queue (MSMQ) folders from virus scanning:

```
%SystemRoot%\system32\MSMQ
%SystemRoot%\system32\MSMQ\storage
```

Configuring WaveNet

To configure WaveNet, you use the WaveNet Management applet, available on the Applications tab of the Global Administrator Management Console.

This section describes how to do the following:

- Adding a Wave Server to the WaveNet network. See page 25-14.
- Testing connections between WaveNet nodes. See page 25-17.
- Publishing local users on remote nodes. See page 25-20.
- Viewing subscribed users. See page 25-23.

Adding a Wave Server to the WaveNet network

You can add your local Wave Server or any other Wave Server to the WaveNet network, or create a new WaveNet network by adding each Wave Server.

To add a Wave Server to the WaveNet network, you add it to one other node according to the following instructions. When a node is added to one node, it is automatically joined to all other nodes that are already connected.

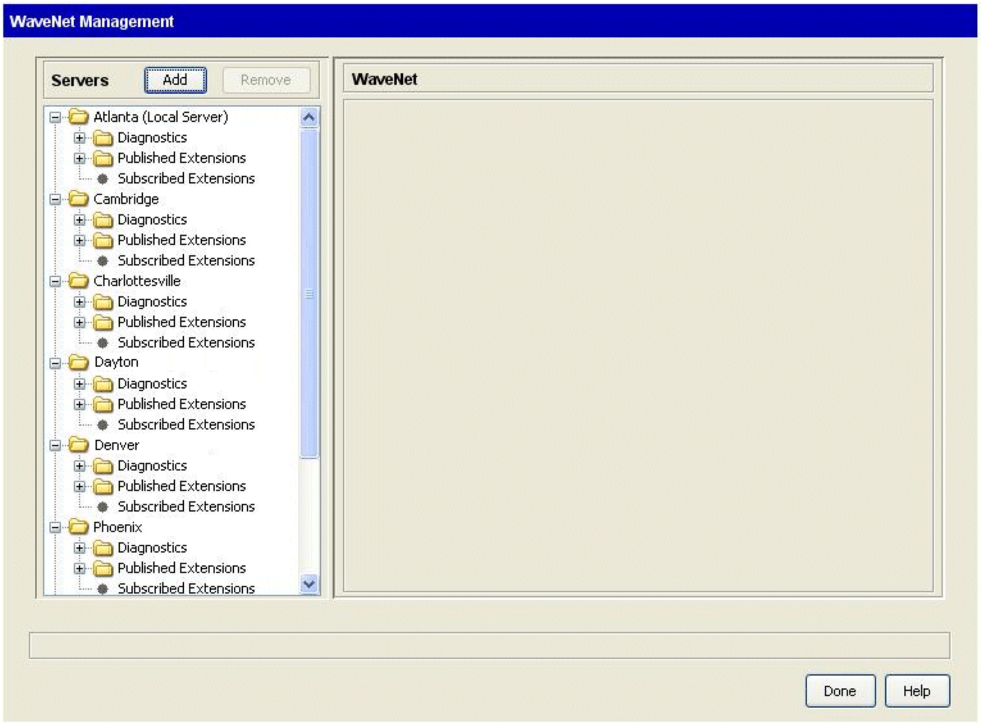
To add your Wave Server to the WaveNet network

1 If necessary, click the Applications tab of the Management Console.

Click

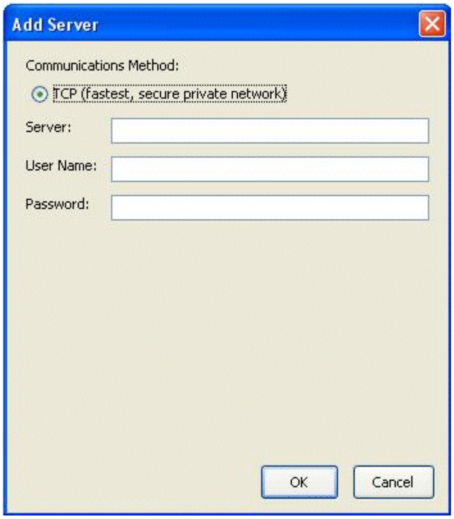
2 Click the WaveNet Settings icon, located in the WaveNet section.

The WaveNet Management screen opens:



The Wave Servers that have already been added to the WaveNet network are listed in the left pane. The Wave Server to which you are running WaveNet Management is identified as "(Local Server)".

3 To add a Wave Server to the WaveNet network, click **Add**. The Add Server dialog opens:



4 Enter the following information:

- **Communications Method**. Select **TCP**.
- **Server**. Enter the Wave Server’s name or IP address.
- **Username** and **Password**. Enter valid Enterprise logon account credentials:
  - **If you are adding your local Wave Server to an existing WaveNet network**, enter Enterprise logon account credentials from any other node in the network.
  - **If you building a new WaveNet network**, enter Enterprise logon account credentials for the Wave Server that you are adding.

5 Click **OK**. The new Wave Server is displayed in the left pane.

If the Wave Server cannot be added to the network, one of the following error messages is displayed.

Note: The actual text of these error message may change by the time that WaveNet is officially released.

Error Message	Cause/Action
Unable to add requested server: Invalid user name or password	The Wave Server cannot be added to the WaveNet network, because the user name and/or password entered in the Add Server dialog are invalid, or that account does not have Enterprise-level rights. Retry using correct account information, or another account with Enterprise-level rights.
Invalid host name.	The Wave Server cannot be added to the WaveNet network, because the Wave Server's name or IP address entered in the Add Server dialog is invalid. Try again using the correct host name.
Maximum number of WaveNet servers are connected to destination.	The Wave Server cannot be added because the current maximum of 100 Wave Servers per WaveNet network has been reached. You cannot add another Wave Server to the WaveNet network until you remove one of the existing nodes.

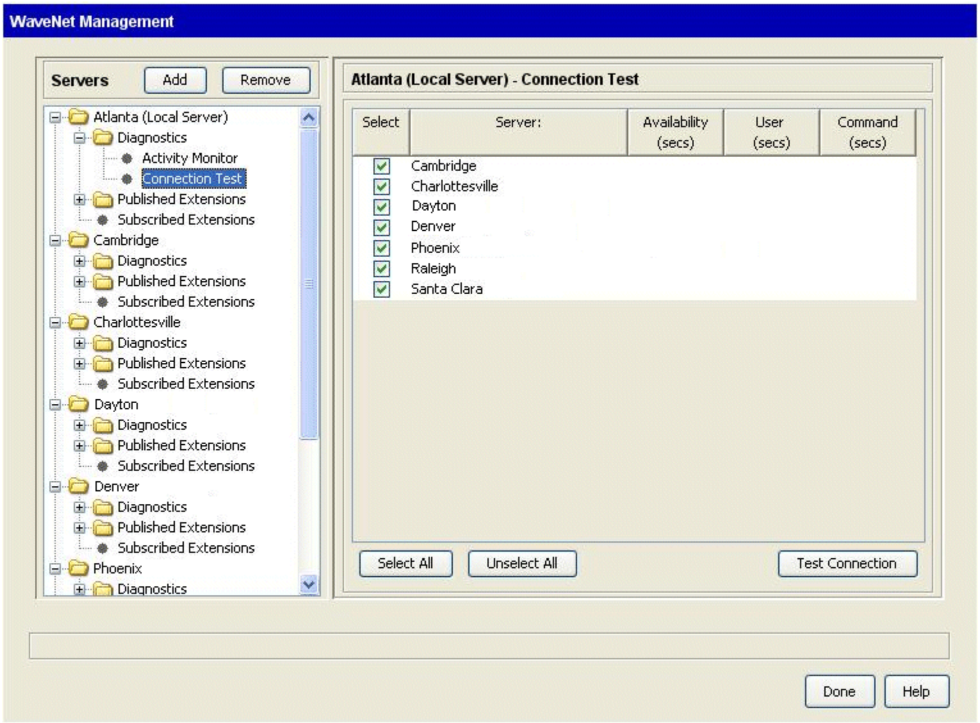
Testing connections between WaveNet nodes

You can test the connection between any two WaveNet nodes from any node in the WaveNet network.

To test the connections between WaveNet nodes

1. To test the connection between your local node and one or more remote nodes, select the local Wave Server in the left pane of the WaveNet Management screen.
2. Expand **Diagnostics** for the selected Server.

3 Click **Connection Test**. The nodes connected to the selected Wave Server are listed in the right pane.

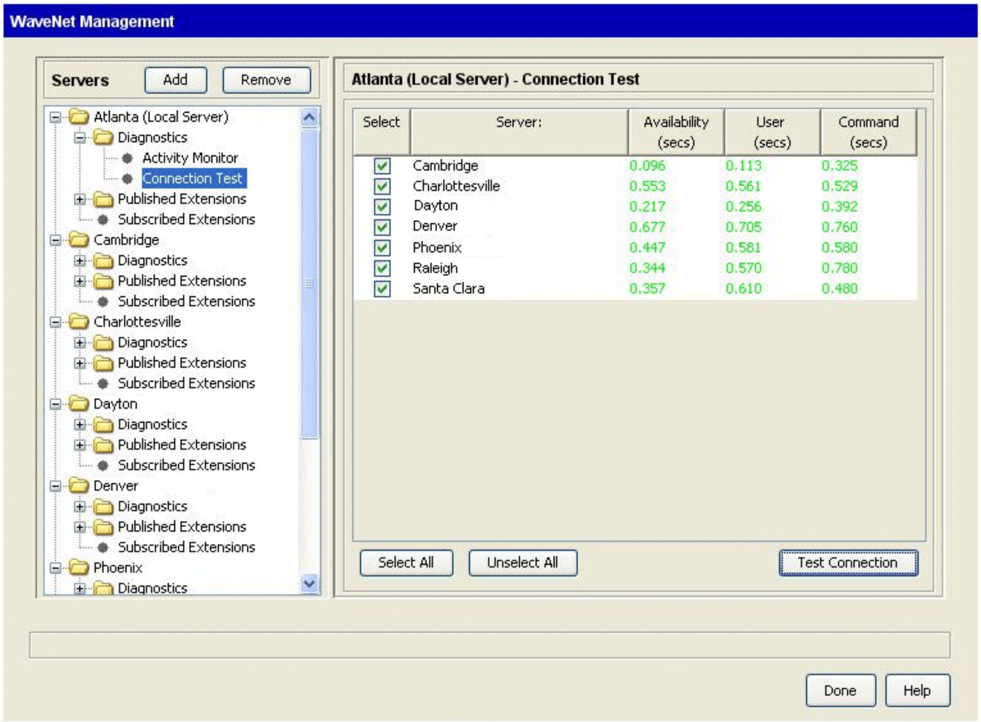


Atlanta (Local Server) - Connection Test

Select	Server:	Availability (secs)	User (secs)	Command (secs)
☑	Cambridge			
☑	Charlottesville			
☑	Dayton			
☑	Denver			
☑	Phoenix			
☑	Raleigh			
☑	Santa Clara			

4 Select the checkboxes for each connection that you want to test. Click **Select All** to test all of the connections displayed.

5 Click **Test Connection**. The right pane is updated with the results of the test:



Atlanta (Local Server) - Connection Test

Select	Server:	Availability (secs)	User (secs)	Command (secs)
☑	Cambridge	0.096	0.113	0.325
☑	Charlottesville	0.553	0.561	0.529
☑	Dayton	0.217	0.256	0.392
☑	Denver	0.677	0.705	0.760
☑	Phoenix	0.447	0.581	0.580
☑	Raleigh	0.344	0.570	0.780
☑	Santa Clara	0.357	0.610	0.480

Response time indicates in milliseconds the time that it took for a test message to be sent round-trip between the testing and responding node:

- **Green**. Connection is functioning normally.
- **Yellow**. Connection is slow.
- **Red**. Connection timed out.

Response times are shown for the following types of separate communications between WaveNet modes:

- **Availability**. On-hook, off-hook, and ringing changes for Gateway users.
- **User**. User information about Gateway users (names, titles, greetings, personal status, contacts, and so forth). This information is sent when users are first published and if the information changes later.
- **Command**. WaveNet administrative commands (Join, Delete, Publish, Unpublish, Test Connectivity, Activity, and so forth) between nodes.

6 Resolve any issues or timeouts identified. For example:
   - Check that non-WaveNet network communications to the affected Wave Servers are functioning normally.
   - Verify that the problem Wave Servers are up and running.
   - Verify that WaveNet is running correctly (not stopped, no errors, and so forth) on the problem nodes.

7 Select another Wave Server in the left pane and repeat these steps to test the connections between that node and other nodes.

Publishing local users on remote nodes

You can publish local users from any Wave Server displayed in the left pane of the WaveNet Management applet to one or more other nodes.

Once a user has been successfully published, that user will be displayed in the **Subscribed Extensions** list for each node that you specified. Note that even though you publish users via a named extension group, the users are listed individually in the Subscribed Extensions list.

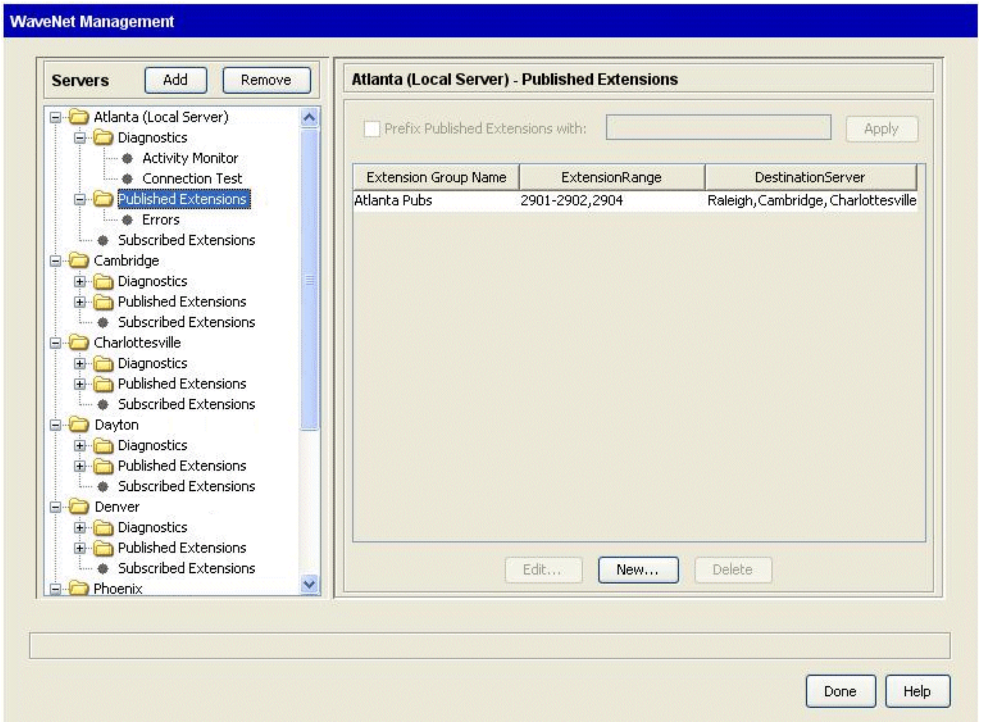
How publishing requests are processed

A new publication request is queued on the home node of the user to be published to other nodes. WaveNet operates at a relatively lower priority than call processing on a Wave Server. On a quiet system or network without much phone activity, publication will complete almost instantaneously. On a very busy system or network, there may be some delay before publication is complete, with subscribed Gateway users displayed for remote nodes and any errors displayed in the Publication Error list for the Gateway user’s home node.

To publish local users as Gateway Users on remote nodes

1 In the left pane of the WaveNet Management screen, select the Wave Server from which you want to publish users.

2 Select **Published Extensions**. Any users that have already been published from this Wave Server are listed in the right pane.



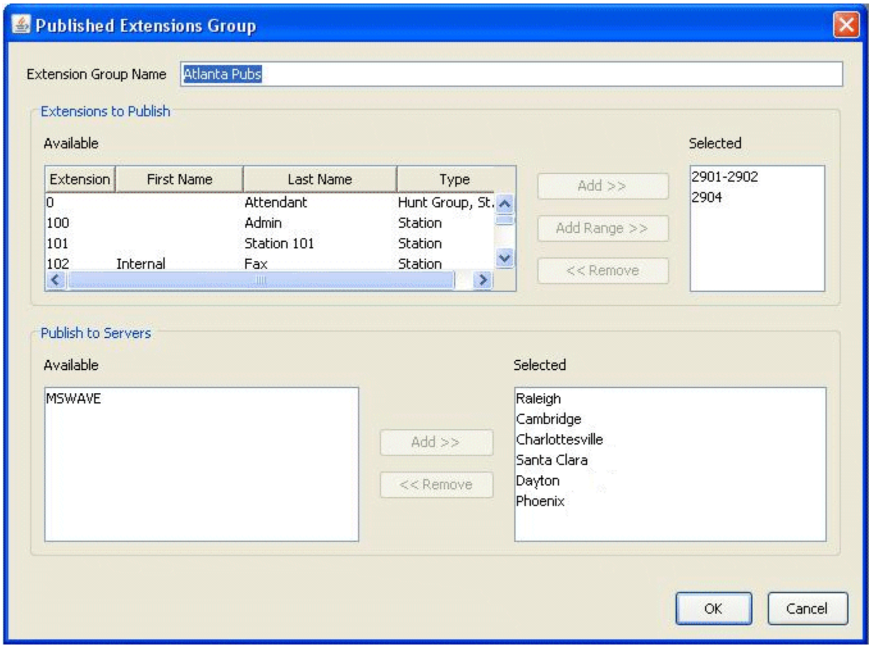
□ Prefix Published Extensions with:

Extension Group Name	ExtensionRange	DestinationServer
Atlanta Pubs	2901-2902,2904	Raleigh,Cambridge,Charlottesville

For those users, the following information is displayed:

- **Extension Group Name**. Name you specified when you created the list of users to publish.
- **Extension Range**. Extensions you added to the Extension Group.
- **Destination Server**. Node to which the users were published.

3 Click **New**. The Published Extensions Group dialog opens:



Published Extensions Group

Extension Group Name: Atlanta Pubs

Extensions to Publish

Available

Extension	First Name	Last Name	Type
0		Attendant	Hunt Group, St.
100		Admin	Station
101		Station 101	Station
102	Internal	Fax	Station

Selected:
2901-2902
2904

Publish to Servers

Available:
MSWAVE

Selected:
Raleigh
Cambridge
Charlottesville
Santa Clara
Dayton
Phoenix

4 Enter the following information:

- **Extension Group Name**. Name of the group of extensions to publish.
- **Extensions to Publish**. List of extensions to publish.
- **Publish to Servers**. Wave Servers where the selected users will be published.

5 Click **OK**.

6 In the left pane, expand **Published Extensions**, and then click **Errors** to see if any publication requests were rejected because of First Digit or extension conflicts. Since publication may not complete immediately on a very busy system or network, click **Refresh Now** to refresh the information displayed in the right pane.

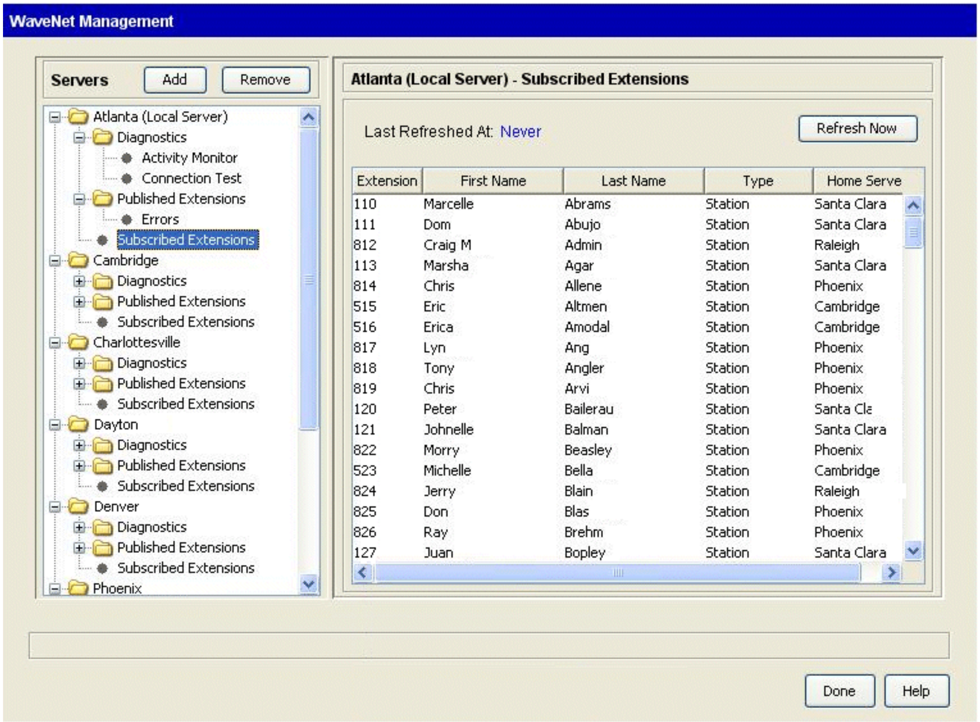
For information about how to resolve publication errors, see “Resolving publication errors” on page 25-24. After you resolve any errors, select an entry and click **Retry**. If there is no longer any conflict, the entry is removed from the table.

Viewing subscribed users

To view the users that have been published to a WaveNet node

1 In the left pane of WaveNet Management screen, select a Wave Server.

2 Select **Subscribed Extensions**. Any users that have already been published to this Wave Server are listed in the right pane.



Atlanta (Local Server) - Subscribed Extensions

Last Refreshed At: Never

Extension	First Name	Last Name	Type	Home Serve
110	Marcelle	Abrams	Station	Santa Clara
111	Dom	Abujo	Station	Santa Clara
812	Craig M	Admin	Station	Raleigh
113	Marsha	Agar	Station	Santa Clara
814	Chris	Allene	Station	Phoenix
515	Eric	Altmen	Station	Cambridge
516	Erica	Amodal	Station	Cambridge
817	Lyn	Ang	Station	Phoenix
818	Tony	Angler	Station	Phoenix
819	Chris	Arvi	Station	Phoenix
120	Peter	Bailerau	Station	Santa Cla
121	Johnelle	Balman	Station	Santa Clara
822	Morry	Beasley	Station	Phoenix
523	Michelle	Bella	Station	Cambridge
824	Jerry	Blain	Station	Raleigh
825	Don	Blas	Station	Phoenix
826	Ray	Brehm	Station	Phoenix
127	Juan	Bopley	Station	Santa Clara

For those users, the following information is displayed:

- **Extension**.
- **First Name, Last Name**.
- **Type**. Station, Auto Attendant, and so forth.
- **Home Server**. Node from which the users were published.

Resolving publication errors

A First Digit or extension conflict can cause a publication request to be rejected with one of the errors listed below. To display these errors, in the left pane expand **Published Extensions** for a node, and then click **Errors**.

Error	Cause/Action
Extension already exists at destination.	The Gateway user cannot be created on the subscribing node because the extension number already exists on that Wave Server. See "Dial plan considerations" on page 25-7 for more about extension conflicts. Resolve the extension conflict and retry.
First/Last name combination already exists at destination.	The Gateway user cannot be created on the subscribing node because a user with the same first and last name already exists on that Wave Server. Resolve the conflict and retry.
Maximum subscribed extension limit reached at destination.	The Gateway user cannot be created on the subscribing node because the current maximum of 1500 GateWay user subscriptions per Wave Server has been reached. You cannot create another Gateway user on the subscribing node until you delete one of the existing Gateway users.
User Exception - First Digit Length.	The Gateway user cannot be created on the subscribing node because the first digit of the user's extension is currently defined in the First Digit Table and is set to **Extension**, but the length of the user's extension does not match the extension length for the user's first digit in the First Digit Table. See "First Digit Table issues" on page 25-8 for more information. Correct the first digit conflict and retry.
User Exception - Already in Use.	The Gateway user cannot be created on the subscribing node because the first digit of the user's extension is currently defined in the First Digit Table, but is set to **Attendant** or **External**. See "First Digit Table issues" on page 25-8 for more information. Correct the first digit conflict and retry.

Using the WaveNet Activity Monitor

The WaveNet Activity Monitor give you a view into WaveNet activity. This information helps you monitor WaveNet's communication activity with other nodes. You can see when there is normal activity by observing the counters increasing, and you can also tell when there might be a problem, if the counters are not increasing normally. If you think you have a problem, observing which counters are moving and which are not can help you troubleshoot the problem, or at least provide you with some details to include when you report the problem to your Technical Support representative.

The WaveNet Activity Monitor tracks the following counters for each WaveNet node:

- **PendingVoicemails**. Number of voicemails on the selected node that have not been sent to the destination node(s) for whatever reason (for example, a communications failure between nodes).
- **ReceivedAvailabilities**. Number of availability changes for subscribed (incoming) GateWay users that the selected node has received. (Each Wave extension can be in one of 3 availability states, OnHook, OffHook, or Ringing.)
- **ReceivedUserUpdates**. Number of user updates for subscribed (incoming) GateWay users that the selected node has received. (A user update could be a change in a user's information, for example name, address, and so forth.)
- **ReceivedVoiceMails**. Number of voicemail messages for local users that the selected node has received.
- **SentAvailabilities**. Number of availability changes for local users that WaveNet has sent to other subscribing nodes.
- **Sent UserUpdates**. Number of user updates for local users that WaveNet has sent to other subscribing nodes.
- **Sent Voicemails**. Number of voicemail messages for Gateway user mailboxes that the selected node has received. (These messages were sent "home" to the node that owns that mailbox so that the user receives them in his or her home mailbox.)

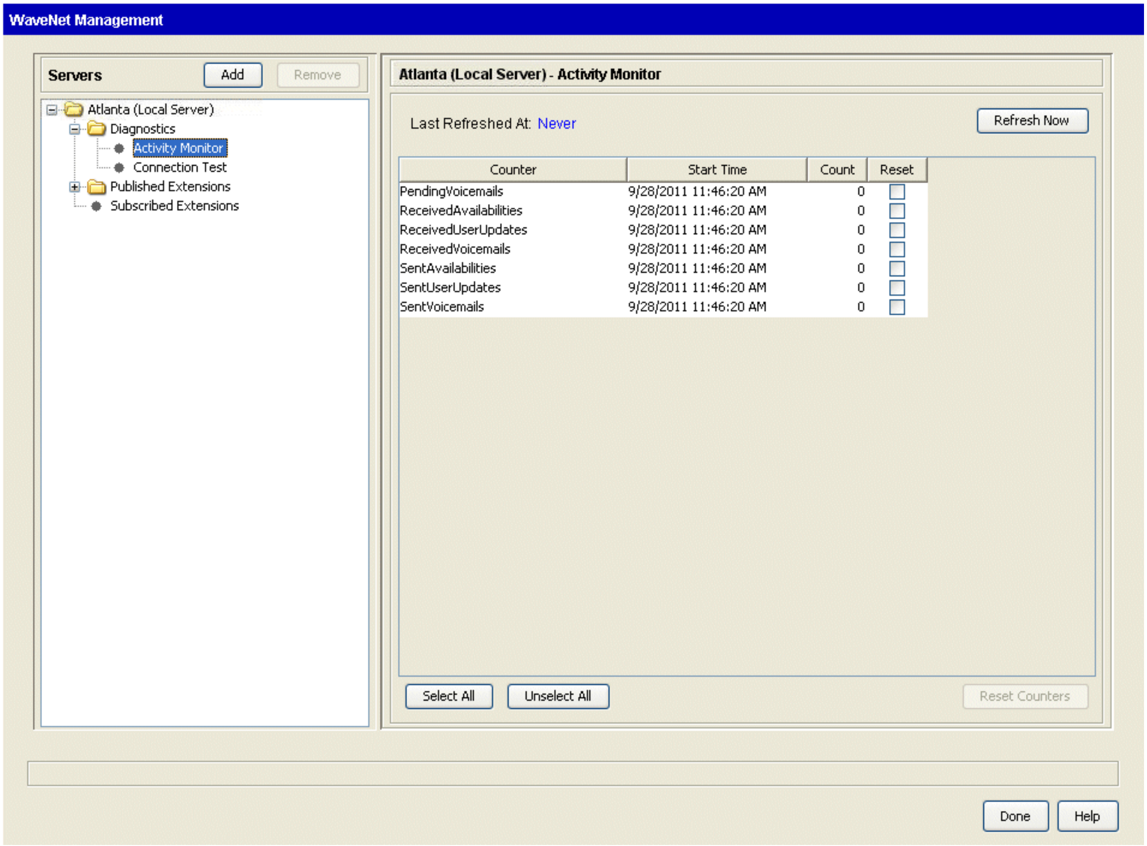
You can inspect the activity counters for any WaveNet node. Refresh the view to see if any of the counters increment. You can force the counters to increment by placing a call as a published user, or call or send a voice mail to a Gateway user.

If the counters do not increment when you know that activity involving a published user or Gateway user should force a change, then WaveNet may not be functioning properly. For example, if you reset the PendingVoicemails counter, WaveNet checks to see it there are any voicemails that need to be sent to another node, and if so, sends them.

To view the WaveNet Activity Monitor

1 In the left pane of the WaveNet Management screen, select the Wave Server whose activity counters you want to view.

2 Select **Diagnostics > Activity Monitor**. The activity counters for this this WaveNet node are listed in the right pane, along with the date and time when the counter was last reset.



Atlanta (Local Server) - Activity Monitor

Last Refreshed At: Never

Counter	Start Time	Count	Reset
PendingVoicemails	9/28/2011 11:46:20 AM	0	☐
ReceivedAvailabilities	9/28/2011 11:46:20 AM	0	☐
ReceivedUserUpdates	9/28/2011 11:46:20 AM	0	☐
ReceivedVoicemails	9/28/2011 11:46:20 AM	0	☐
SentAvailabilities	9/28/2011 11:46:20 AM	0	☐
SentUserUpdates	9/28/2011 11:46:20 AM	0	☐
SentVoicemails	9/28/2011 11:46:20 AM	0	☐

Do any of the following:

- Click **Refresh Now** to update the counters at any time.
- To reset the one to more counters to zero, select each counter’s **Reset** checkbox and then click **Reset Counters**. To reset all of the counters, click **Select All** first.

Chapter 26

Using the Call Classifier

CHAPTER CONTENTS

The Wave Call Classifier add-on allows you to create rules to identify callers, intelligently route calls, and present Contact Center agents with scripts and related caller information before calls are answered. Creating Call Classifier rules is part of auto attendant configuration, and you can create as many rules as you want per auto attendant.

The Call Classifier can query any ODBC-compliant database (Microsoft Access, SQL Server, Excel, Oracle database, and so forth) in order to display detailed caller information on agents' screens. In addition, by verifying caller data, the Call Classifier can route callers to the agent best equipped to handle each call.

How to use the Call Classifier to customize inbound call handling

The following examples provide some ideas on how to use the Call Classifier:

- Set a caller's queue priority based on issue number, customer number, or Caller ID to bump them up in line.
- Get detailed profile information on any business or end user from any ODBC database.
- Prompt callers for any numeric information, and validate it based on any ODBC database, then send the resulting profile information to the agent.
- Prevent non-validated callers from reaching an agent.
- Based on the area code that the customer is calling from, route callers to the agents most appropriate for that region.
- Based on your own custom or company database, attach issue numbers, customer profiles, addresses, and other information to the call when customers call.
- Add agent call scripts (with optional embedded customer name) to the Call Notes based on Caller ID and a custom database query (for example, “Is Mr. Jones available? This is Fred Holmes from XYZ Corp…”).
- Add Caller ID name where none exists by looking up the Caller ID number in a white pages database or database of area codes and regions.
- Add meaning to DID numbers. For example, ABC corp has a different support phone number (using DID) for each of their products. As the Call Classifier receives calls, it can add the appropriate product name to the Notes field based on DID, then route the call to the support queue. Agents using the Call Monitor can see the product name before answering the call, resulting in a shorter call and a more informed agent.
- In conjunction with Wave Fax Manager, allow a single DID number to be used for both faxes and calls. Use Wave auto attendants for fax detection, and then use the Call Classifier to route calls to users if no fax is detected.
- Create a global “black list” so that all calls from a set of particular numbers are sent directly to voice mail or are disconnected.
- Hide certain or all Caller IDs from users by setting Caller ID to nothing.
- Add address information to calls based on Caller ID. If Caller ID isn't present, you can have the Call Classifier prompt the caller for their phone number.

How the Call Classifier works

The Call Classifier can recognize incoming calls based on any of the following:

- DID (the phone number dialed by the caller)
- Caller ID name or number
- Call Notes
- Account code
- Custom data
- Skill

Call recognition can be based on a match on:

- Any number or text that you enter in a Call Classifier rule
- A record in your company's ODBC database

Once a call is recognized, you can perform the following actions:

- Route the call to an extension or voice mailbox.
- Populate the Call Notes field with custom information.
- Replace the DID number, Caller ID number, Caller code with text of your choice.
- Set or reset Custom Data variables attached to the call.
- Hang up on the call.
- Process additional Call Classifier rules.

Call Classifier requirements

Once your Wave Server meets the requirements listed below, the Call Classifier functionality for Wave auto attendants will be operational—no additional installation steps are required.

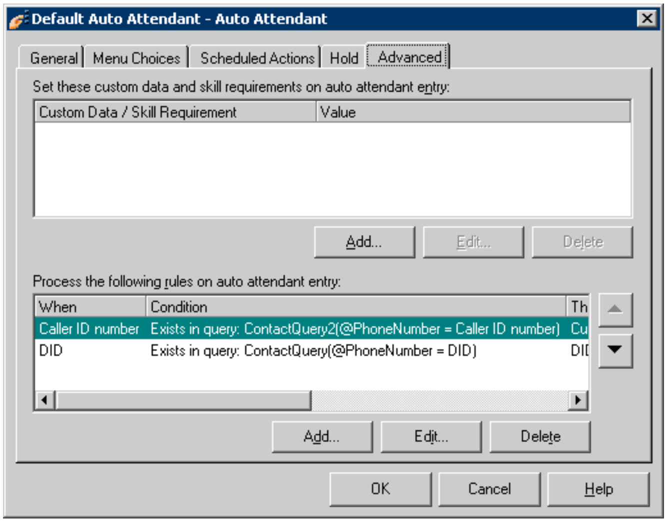
Make sure that each Wave Server where you plan to run the Call Classifier meets the following requirements:

- Install or upgrade the Wave Server to the required versions. For the latest information, contact your Vertical provider.
- Purchase, enter, and activate required one Call Classifier license per Wave Server. For more about Wave licenses, see Chapter 24.

Viewing Call Classifier rules

Perform the following steps to view Call Classifier rules already associated with an auto attendant.

1. In the Auto Attendants view, double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.
2. Click the Advanced tab. Call Classifier rules that have been defined so far are displayed in the **Process the following rules on auto attendant entry** section at the bottom of the dialog. In the following example, 2 rules have been defined for the default auto attendant:



Set these custom data and skill requirements on auto attendant entry:

Custom Data / Skill Requirement	Value

Process the following rules on auto attendant entry:

When	Condition	Th
Caller ID number	Exists in query: ContactQuery2(@PhoneNumber = Caller ID number)	Cu
DID	Exists in query: ContactQuery(@PhoneNumber = DID)	DII

The following information is displayed for each Call Classifier rule. Use the scroll bar to view all of the columns.

- **When**. Description of the attribute on which to base the rule.
- **Condition**. Summary of the condition. The valid conditions are:
  - Matches: <value>
  - Does not match: <value>
  - Starts with: <value>
  - Does not start with: <value>
  - Exists in query: <value>
- **Then change**. Summary of all changes performed by the rule, as in:
  - Change <field> to <value>, <field> to <value>, etc.
- **And then**. Final action summary. The valid final actions are:
  - Transfer to extension
  - Continue to next rule
  - Send to voice mail
  - Continue with auto attendant
  - Hang up
  - Transfer to extension (from query)
  - Send to voice mail (from query)

Ordering rules in the Call Classifier dialog

You can have the Call Classifier apply several rules to a call in sequence. For example, the first rule could identify support calls by DID and attach the name of the product to the DID field, then the second rule could take the Caller ID and search your database to find the date of this customer’s last call, attaching that information to the Call Notes field. In order to have a rule process a call after another rule, make sure the rules are listed with the first rule to be processed at the top and the last rule to be processed at the bottom.

In the case of conflicts between rules, the highest-listed rule will be used first. For example, you have two call rules, one that handles calls from Caller ID (617) 555-1212 and one that handles calls to DID 5001. If a call comes in with Caller ID (617) 555-1212 *and* DID 5001, the call will be handled by whichever rule is listed first.

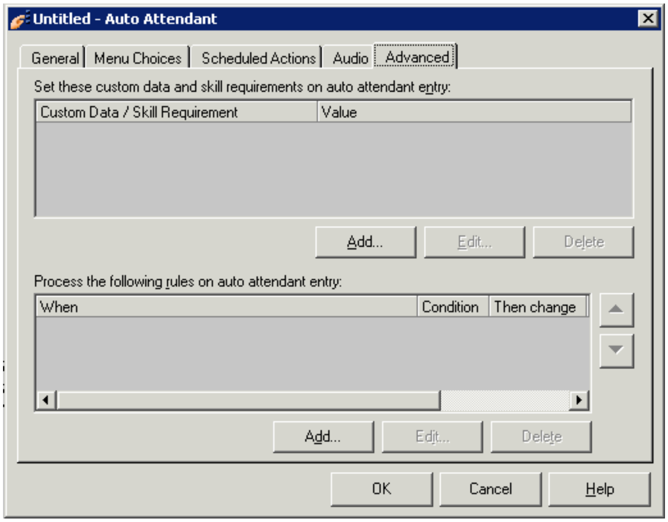
To reorder a Call Classifier rule in the list, select it and then click the **Up** or **Down** arrow button.

Adding a Call Classifier rule to an auto attendant

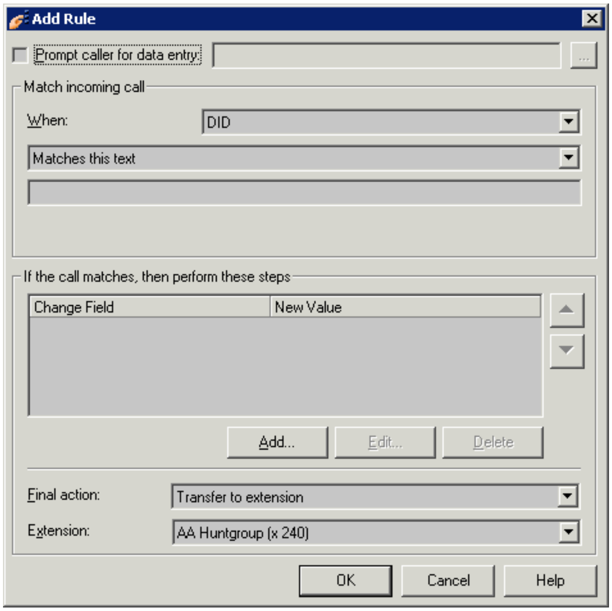
Note: If no valid Call Classifier license is detected on the Wave Server, the fields described in the following steps are disabled.

1 In the Auto Attendants view, create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.

2 Click the Advanced tab.


Untitled - Auto Attendant
General
Menu Choices
Scheduled Actions
Audio
Advanced
Set these custom data and skill requirements on auto attendant entry:
Custom Data / Skill Requirement
Value
Add...
Edit...
Delete
Process the following rules on auto attendant entry:
When
Condition
Then change
Add...
Edit...
Delete
OK
Cancel
Help

3 In the **Process the following rules on auto attendant entry** section, click **Add** to create a new rule (or select an existing rule and click **Edit** to modify it). The Add Rule dialog opens:


Add Rule
□ Prompt caller for data entry
Match incoming call
When: DID
Matches this text
If the call matches, then perform these steps
Change Field
New Value
Add...
Edit...
Delete
Final action: Transfer to extension
Extension: AA Huntgroup (x 240)
OK
Cancel
Help

4 Select the **Prompt caller for data entry** checkbox to prompt callers to enter an identifying number, such as their phone number, account number, or support issue number. See “Prompting the caller to enter an identifying number” on page 26-10 for more information on how to record the prompt that you want callers to hear, set up validation and database matching, and so forth.

5 In the **Match incoming call** section, define when an incoming call will be affected by this rule:

a Select one of the following attributes by which to recognize an incoming call from the drop-down list:

- **DID**
- **Caller ID number**
- **Caller ID name**
- **Call notes**
- **Account code**
- **Custom data**
- **Skill**

b Select one of the following conditions from the drop-down list:

- **Matches this text**
- **Does not match this text**
- **Begins with this text**
- **Does not begin with this text**
- **Exists in this custom database query**

Note: Configuring a rule that includes a custom database query requires additional steps. See “Using custom database queries in Call Classifier rules” on page 26-13.

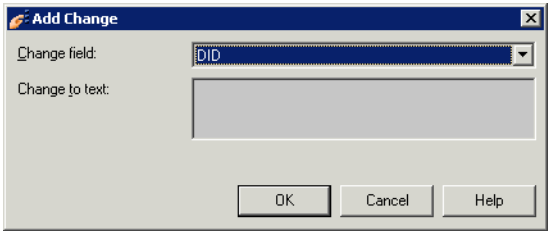
c Enter the text to compare on in the text box.

6 In the **If the call matches, then perform these steps** section, you define the steps that will occur if the incoming call matches the condition, for example setting a custom variable, adding call notes, and so forth. A rule can contain one or more steps.

Click **Add** to create a new step (or select an existing step and click **Edit** to modify it). The Add Change dialog opens:

7 Select the **Change field** from the drop-down list. Depending on the **Change field** that you select, you will need to enter the following information:

- **DID**, **Caller ID number**, **Caller ID name**, **Call notes**, **Account code**. Enter the **Change to text**. The specified field will be updated with the text that you enter here.

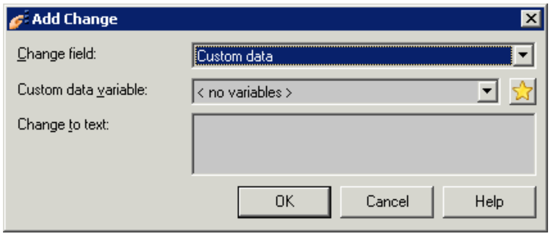


Change field: DID

Change to text:

- **Custom data**. Select the **Custom data variable** to modify from the drop-down list, or click ☆ to create a new custom variable. (For more about creating and using custom data variables, see Chapter 2 in the *Wave Contact Center Administrator Guide*.)

Enter the **Change to text**. The custom data variable will be updated with the text that you enter here.



Add Change

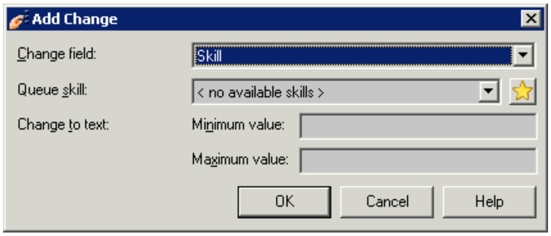
Change field: Custom data

Custom data variable: < no variables >

Change to text:

- **Skill**. Select the **Queue skill** to attach as a requirement to the call from the drop-down list, or click ☆ to create a new skill. (For more about creating and using skill requirements for call routing, see Chapter 3 in the *Wave Contact Center Administrator Guide*.)

  For **Minimum value** and **Maximum value**, enter the range (from 0 to 100) that an agent's skill value must be within to qualify for taking the call.



Add Change

Change field: Skill

Queue skill: < no available skills >

Change to text: Minimum value: Maximum value:

Click **OK** to return to the Add Rule dialog.

8 Select the **Final action** from the drop-down list. This action will be performed after all of the steps in the rule have been performed.

- **Transfer to extension**. Select the **Extension** from the drop-down list.
- **Continue to next rule**. Call processing will continue with the next rule (if any) defined for this auto attendant.
- **Send to voice mail**. Select the **Extension** from the drop-down list.
- **Continue with auto attendant**. Call processing will continue according to this auto attendant's configuration.
- **Hang up**

- **Transfer to extension (from query)**. Select this option to transfer the call to the extension returned by your custom database query, and then select the **Extension** from the drop-down list.
- **Send to voice mail (from query)**. Select this option to transfer the call directly to the extension returned by your custom database query, and then select the **Extension** from the drop-down list.

  Note: See “Using custom database queries in Call Classifier rules” on page 26-13 for more about creating and testing custom database queries.

9 Click **OK** to save the rule and return to the Auto Attendant dialog.

Prompting the caller to enter an identifying number

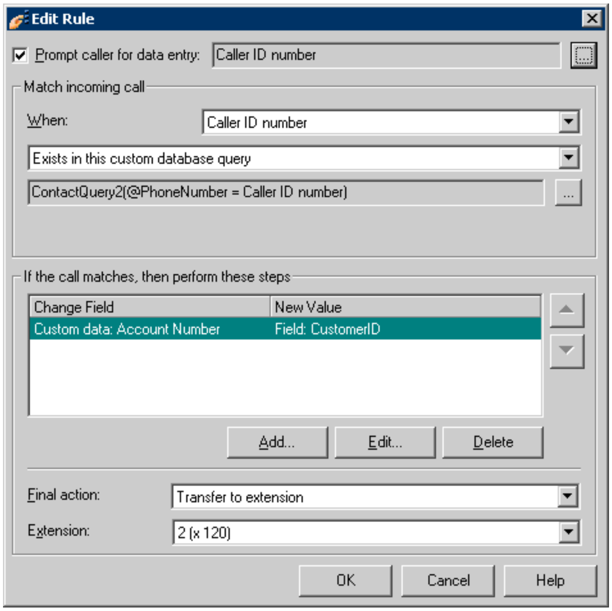
You can have the Call Classifier prompt callers to enter an identifying number, such as their phone number, account number, or support issue number. The Call Classifier can then identify the caller based on that number, and attach the number to the call in any supported field, such as Caller ID, Call Notes, a Custom Data variable, and so forth. The number can then be viewed by the users who answer the call via the ViewPoint Call Monitor.

You can also choose to only prompt the caller for information when it is missing—if the information field is already populated, the caller will not prompted. For example, if you prompt callers to enter a phone number to populate the Caller ID number field, the prompt will be skipped for calls that already contain a Caller ID number. In this way all your calls will have a populated Caller ID field, without disturbing the majority of callers with unnecessary prompts.

Important! Your prompt should remind callers to press # after completing their entry to let the system know they have finished. If the caller doesn't do this, Wave will wait up to 10 seconds for additional input.

To use caller prompting

1 In the Edit Rule dialog, select the **Prompt caller for data entry** checkbox.



Edit Rule

☑ Prompt caller for data entry: Caller ID number

Match incoming call

When: Caller ID number

Exists in this custom database query

ContactQuery2(@PhoneNumber = Caller ID number)

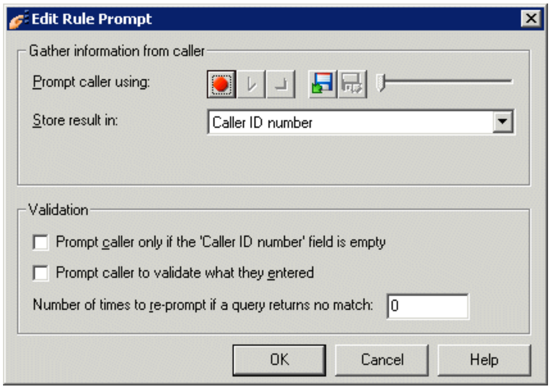
If the call matches, then perform these steps

Change Field	New Value
Custom data: Account Number	Field: CustomerID

Final action: Transfer to extension

Extension: 2 (x 120)

2 Click the ... button. The Edit Rule Prompt dialog opens.



Edit Rule Prompt

Gather information from caller

Prompt caller using:

Store result in: Caller ID number

Validation

☐ Prompt caller only if the 'Caller ID number' field is empty

☐ Prompt caller to validate what they entered

Number of times to re-prompt if a query returns no match: 0

3. In the **Gather information from caller** section, use the audio controls to record the prompt that you want callers to hear (for example, “Please enter your account number, followed by the pound sign”), or import an existing audio file. (See “Using the audio controls” on page 2-21 for details.)

4. From the **Store result in** drop-down list, choose one of the following fields in which to store the information provided by the caller in response to the prompt.

   Note: Any data already in the field will be overwritten.

   - **Caller ID number**
   - **Call notes**
   - **Account code**
   - **Custom data**. If you choose this option, select an existing **Custom data variable** from the drop-down list, or click ☆ to create a new custom variable. (For more about creating and using custom data variables, see Chapter 2 in the *Wave Contact Center Administrator Guide*.)

5. In the **Validation** section, to use caller prompting only when the desired information is not present, select the **Prompt caller only if __ is empty** checkbox. For example, if you selected **Caller ID number** in step 4, then the Call Classifier will only prompt callers to enter a number when the Caller ID number field of the call is empty. Callers will not be prompted when there is a number in the Caller ID number field.

   If **Prompt caller only if __ is empty** is not selected, callers are prompted to enter a number, even if a number is already present in the field. Note that any number entered by the caller will overwrite the number that came in with the call.

6. To play the number entered back to the caller, and prompt the caller to confirm it or reenter it, select the **Prompt caller to validate what they entered** checkbox. If **Prompt caller to validate what they entered** is not selected, the number is accepted as entered, without repeating it back to the caller for confirmation.

7. If you are using a custom database query to match the number entered against records in a database (as described in “Using custom database queries in Call Classifier rules” on page 26-13), you can respond to non-matches by prompting the caller to reenter the number.

   For example, if every incoming caller must have a valid issue number, and a caller’s issue number does not exist in your Issues database, you can configure the Call Classifier to prompt the caller to reenter it. The reenter prompt is repeated on failed matches for the number of times that you specify. If there is still no match, the call continues with no change to the field that would have been updated.

   To use this feature, enter the **Number of times to re-prompt if a query returns no match**. If you do not want to reprompt callers if no match is found, set this field to 0.

Using custom database queries in Call Classifier rules

You can use custom database queries in Call Classifier rules to query your existing databases to identify callers, and then attach information to calls or transfer callers to different extensions based on the results of the database query.

For example, you could compare the incoming Caller ID number to all the phone numbers in your contact database. If there is a match, you could then add information to the Call Notes associated with the call from that contact record, for example the date and order number of the customer's last purchase. The agent taking the call will then see that information in the Notes pane of the ViewPoint Call Monitor.

The Call Classifier can query any Microsoft OLE DB supported database, for example Microsoft Access, SQL Server, Excel, Oracle, and so forth. For proper operation, this database should NOT be on the Wave Server. You can make an ODBC connection with a database on a server on your network.

There are two ways to perform a custom database query:

- With a stored procedure or MS Access query. With this option, you specify the name of a stored procedure or query that you have created in your database.
- With a dynamic SQL query. With this option, you specify a full dynamic SQL "Select" statement.

Using a custom database query in a Call Classifier rule consists of the following tasks:

- Configuring each database connection as a system data source via the Windows ODBC Data Source Administrator (**Control Panel > Settings > Admin Tools > Data Sources (ODBC)**). For details on how to add a system data source, see the ODBC Data Source Administrator Help.

  Caution! *Several Vertical system data sources may be listed in the ODBC Data Source Administrator, for example "InstantOffice_Hardware", "InstantOffice_IOAgent", "IACDRep", "CMSDatabase", "CRQLog", "CallRecorder_DSN", and so forth. Do NOT modify these data sources.*

- Defining and testing the database query. See page 26-14.
- Attaching the query results to the call as data. See page 26-18.
- Routing the call based on the query result. See page 26-19.

Defining and testing the database query

1 In the Auto Attendants view, create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog opens.

2 Click the Advanced tab.

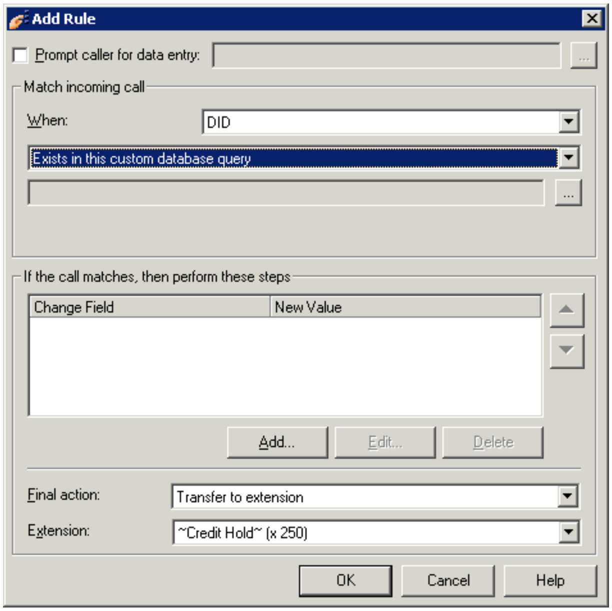
3 In the **Process the following rules on auto attendant entry** section, click **Add** to create a new rule (or select an existing rule and click **Edit** to modify it). The Add Rule dialog opens.

4 In the **Match incoming call** section, define when an incoming call will be affected by this rule:

   a Select one of the following attributes by which to recognize an incoming call from the drop-down list:

   - **DID**
   - **Caller ID number** or **Caller ID name**
   - **Call notes**
   - **Account code**
   - **Custom data**
   - **Skill**

   b Select **Exists in this custom database query** from the drop-down list.


Add Rule

□ Prompt caller for data entry:

Match incoming call

When: DID

Exists in this custom database query

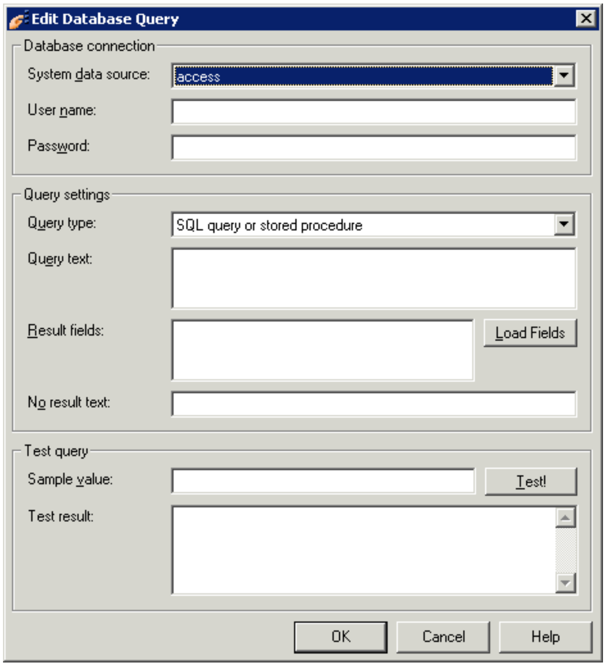
If the call matches, then perform these steps

Change Field	New Value

Final action: Transfer to extension

Extension: ~Credit Hold~ (x 250)

5 Click ... to open the Edit Database Query dialog.



System data source: access

Query type: SQL query or stored procedure

6 In the **Database connection** section, select the database that you want to query from the **System data source** drop-down list. (You must have previously configured your database connections as system data sources via the Windows ODBC Data Source Administrator before they will be listed here. See your Windows documentation for more information.)

Caution! *Several Vertical system data sources may be listed in the System data source drop-down list, for example “InstantOffice_Hardware”, “InstantOffice_IOAgent”, “IACDRep”, “CMSDatabase”, “CRQLog”, “CallRecorder_DSN”, and so forth. Do NOT select these data sources.*

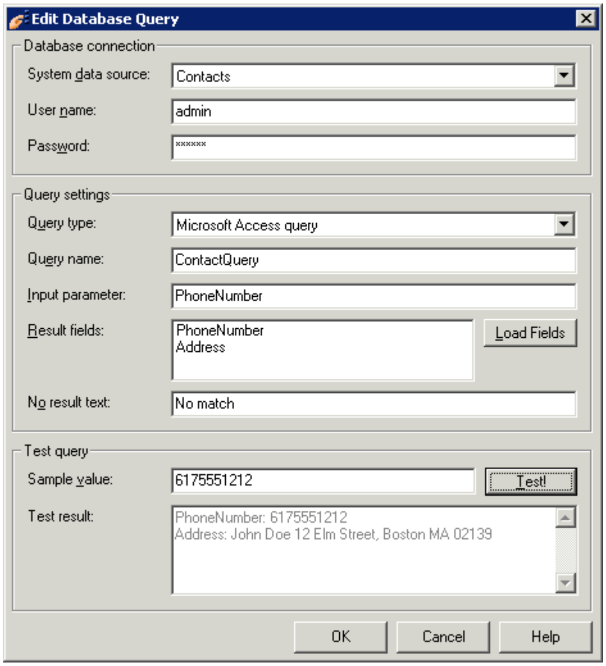
7 Enter the **Username** and **Password** required to access the selected database. Leave these fields blank if no user name or password is required.

8 In the **Query settings** section, select the **Query type**:

- **Microsoft Access query**. With this option, the Call Classifier queries your database using a custom stored procedure or query within the database. To use this option, you must first create the stored procedure or query, as described in “Setting up a stored procedure or query in your database” on page 26-20.

  Enter the following information:

- **Query name**. Enter the name of your query, for example “CallerID Query”. The name must match exactly for the query to work.
- **Input parameter**. Enter the name of the input parameter expected by your query, for example “PhoneNumber”. The name must match exactly for the query to work.



Edit Database Query

Database connection

System data source: Contacts

User name: admin

Password: ******

Query settings

Query type: Microsoft Access query

Query name: ContactQuery

Input parameter: PhoneNumber

Result fields: PhoneNumber
Address

No result text: No match

Test query

Sample value: 6175551212

Test result: PhoneNumber: 6175551212
Address: John Doe 12 Elm Street, Boston MA 02139

Go to step 9.

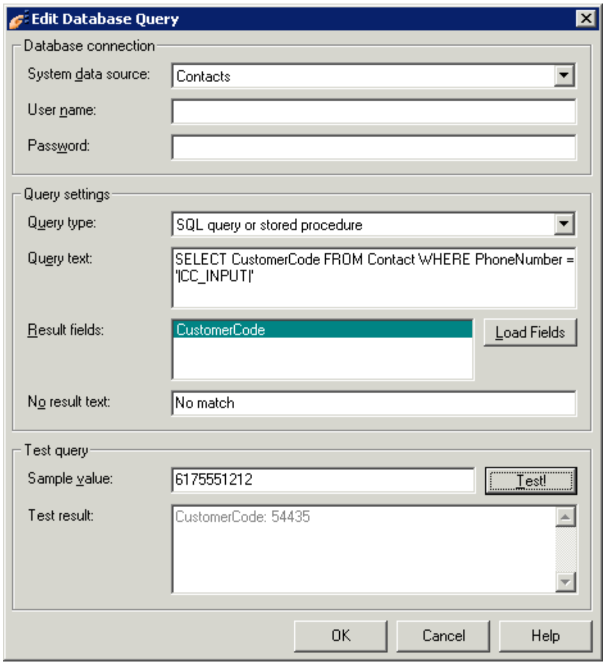
- **SQL query or stored procedure**. With this option, the Call Classifier queries your database using a dynamic SQL query that you specify here, or a custom stored procedure or query within the database. If the latter, you must first create the stored procedure or query, as described in “Setting up a stored procedure or query in your database” on page 26-20.

  Enter the **Query text**:

  - **For a dynamic SQL Query.** Enter your SQL Select statement. Insert the string |CC_Input| where the input data will go, as in the following example:

    SELECT Field2, Field3 FROM Table1 WHERE Field1 = ‘|CC_Input|’

Note that when you query an SQL database, you can merge multiple fields. For details, see “Merging multiple SQL data fields into a single result field” on page 26-20.



System data source: Contacts
User name:
Password:
Query type: SQL query or stored procedure
Query text: SELECT CustomerCode FROM Contact WHERE PhoneNumber = '|CC_INPUT|'
Result fields: CustomerCode
No result text: No match
Sample value: 6175551212
Test result: CustomerCode: 54435

- **For a query or stored procedure**. Enter the name of your custom stored procedure or query, for example “myStoredProcedure”. The name must match exactly for the query to work.

9 In the **No result text** field, enter the text message to return when no match is found in your database.

Important! This field must be filled in or the query will fail to run.

10 Click **Load Fields** to execute the query and retrieve the names of all fields returned by the query. You will use these field names later to set or change call values (as described in “Attaching the query results to the call as data” on page 26-18.

- **Result fields**. Displays the names of the fields returned from the Query Text. (You must enter text in the **No Result Text** field before the **Load Fields** button will work.)

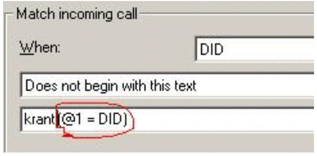
11 In the **Test Query** section, verify that the query works using the following fields:

- **Sample value**. Enter a sample input parameter.
- **Test!**. Click to test the query.
- **Test result**. Displays the result of the query.

If the test query does not succeed, check syntax and spelling. For a stored query or procedure, make sure that the spelling of the Input parameter and each Result field is exactly the same as in the database procedure.

When you have verified that the query works, click **OK** to return to the Add Rule dialog.

Note: After creating a Call Classifier rule that uses an MS Access custom database query, unexpected text may be displayed in the text box below the Condition in the Add Rule dialog. This behavior occurs for any defined condition, as in the following example. This unexpected text is harmless and does not affect the Call Classifier rule in any way.



Match incoming call

When: DID

Does not begin with this text

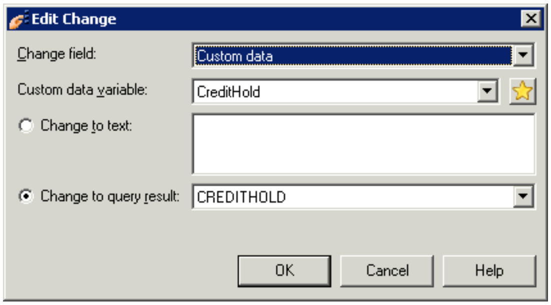
krant{@1 = DID}

12 To finish adding this rule, go to step 6 on page 26-8.

Attaching the query results to the call as data

You can choose to attach one or more of a database query's **Result fields** (as specified in the Edit Database Query dialog) to the call. Any information already in a field (such as a Caller ID number) will be overwritten when this rule executes.

1 In the Add Rule dialog, select the entry for the query in the **If the call matches section**, and then click **Edit**. The Edit Change dialog opens:



Edit Change

Change field: Custom data

Custom data variable: CreditHold

○ Change to text:

● Change to query result: CREDITHOLD

2 In the **Change field** drop-down list, select the field associated with the call that you want to set or change with the results of the database query.

To change the value of a **Custom data variable** with the results of the database query, select it from the drop-down list, or click ☆ to create a new custom variable. (For more about creating and using custom data variables, see Chapter 2 in the *Wave Contact Center Administrator Guide*.) Make sure that the variable type matches the expected result. For example, if the database query returns text information, the variable must be of type String.

3 Select the **Change to query result** checkbox, and then select the query name from the drop-down list.

4 Click **OK** to return to the Edit Rule dialog. If this is a new Call Classifier rule, to finish adding this rule go to step 6 on page 26-8.

Routing the call based on the query result

If your query retrieves an extension number, you can route the call to that extension when the rule executes using the **Final action** drop-down list in the Add/Edit Rule dialog as described in step 8 on page 26-8.

You can route the call so that it rings the extension, or send the call straight to the extension's voice mail. Select either **Transfer to extension (from query)** or **Send to voice mail (from query)**.

Merging multiple SQL data fields into a single result field

When querying a SQL database, you can merge two or more data fields into a single result field. For example, if a customer's address is split across several fields, you can merge them into one result that can then display the full customer address in Call Notes associated with a call.

You can use the merge syntax when specifying a SQL Select statement in the Call Classifier or when creating a stored procedure in the SQL database.

The syntax for merging fields is:

```
Field1 + Field2 <...+ Fieldn> AS NewField
```

where "NewField" is the result field that you then enter in **Result fields**.

You can concatenate spaces, punctuation marks, vertical bars, and other characters in the syntax string to separate the fields.

The following example concatenates an address from several fields into one result:

```
SELECT Street + ' ' + City + ', ' + State + ' ' + Zip AS Address FROM Table1 WHERE
Phone1 = '|CC_Input|'
```

You then enter "Address" in **Result fields**.

Setting up a stored procedure or query in your database

If your Call Classifier rule executes a SQL stored procedure or Microsoft Access query, you must create the stored procedure or query in your database before the Call Classifier can use it.

This section describes how to create a stored procedure using Microsoft SQL Server and a database query using Microsoft Access. To create queries using other databases, refer to the documentation for your database or the Microsoft Access documentation.

Note: This section does not apply to you if your Call Classifier rule executes a dynamic SQL query, as described in "Using custom database queries in Call Classifier rules" on page 26-13.

Creating a SQL stored procedure

This section describes how to create a stored procedure using Microsoft SQL Server for use in a Call Classifier rule. For detailed information, see the Microsoft SQL Server documentation.

- Use a tool such as Microsoft SQL Query Analyzer to open your SQL database and add a new stored procedure.
- Your stored procedure must have a single input parameter that corresponds to the DID, Caller ID Name, Caller ID Number, Call Notes, Account Code, Custom Data, or Skill being passed by the Call Classifier. The stored procedure must return a named recordset. In the following example, the stored procedure is named “myStoredProcedure”, the input parameter is called “@CallerID”, and the returned recordset field is called “Last Order”.

```
CREATE PROCEDURE  myStoredProcedure
  @CallerID as varchar(15)
AS
BEGIN

  SELECT TableName.CompanyName + TableName.LastOrder  as "Last
    Order"
  FROM TableName
  WHERE TableName.PhoneNumber = @CallerID
    END
```

Creating a Microsoft Access query

This section describes how to create a Microsoft Access query for use in a Call Classifier rule. For detailed information, see the Microsoft Access documentation.

- When creating a query, you must add the table or tables that contain the field with the data to which the information from the call (DID, Caller ID, and so forth) will be compared, and the field with the results that you want to attach to the call.
- Similarly, you must add the field with the data to which the information from the call (DID, Caller ID, and so forth) will be compared, and the field with the results that you want to attach to the call.

- Define the name of the input parameter that represents the information sent by the Call Classifier, for example the caller’s phone number. The Call Classifier can send the following input parameters:
  - DID
  - Caller ID Name
  - Caller ID Number
  - Call Notes
  - Account Code
  - Custom Data
  - Skill

Replacing many Call Classifier rules with a database query

As you deploy Call Classifier rules, you may find yourself creating many rules to process individual DID numbers, Caller ID numbers, or other static values, to the point where the number of rules becomes hard to manage. For example, you might have ten or more Call Classifier rules, each processing a different DID number.

As an alternative you can place the values you are checking (DID numbers, Caller IDs, and so forth) in an Microsoft Access table you create, and then use a single Call Classifier rule with a custom database query to perform the same processing as multiple individual rules.

The following example creates a Microsoft Access table and a single Call Classifier rule to look up a caller’s DID and return the extension to which the call will be transferred:

1. Create a table in a Microsoft Access database called “DID” with two fields, “DID” and “Ext”.
2. Populate the table with a row for every DID number, with each row containing the appropriate extension number to which calls to that number should be routed.
3. Create a Access query called “DIDQuery” that takes as input a DID number and returns the corresponding extension number from the DID table.
4. In the Call Classifier, create one rule with a custom database query, that calls the DIDQuery based on the caller’s DID number, then transfers the caller to the extension returned as the query result. See “Creating a Microsoft Access query” on page 26-21 for information about creating a Microsoft Access query.

Viewing Call Classifier information in the Call Monitor

In order for users and agents to view the information attached to calls by the Call Classifier, they must set up the ViewPoint Call Monitor as follows:

- To view Call Notes, make sure the Notes pane is showing by choosing **View > Notes Pane**. (You can also display Call Notes in the Notes column.)
- Make sure that the following columns are displayed in the Call Monitor. To do so, while in the Call Monitor choose **View > Current View > Show Columns**, and then select the relevant column:
  - To view the DID information, make sure the DID column in showing.
  - To view Caller ID number and name, make sure the Number column is showing.
  - To view Custom Data, make sure the appropriate Custom Data column is showing. A Custom Data variable must first be defined as described in “Using custom data variables” on page 20-18 before it will be available in the Show Column list.

Part 3

Key Wave Concepts

Understanding Wave Trunks

Chapter Contents

For configuration procedures related to the concepts in this chapter, see “About creating new trunk groups” on page 5-2 and “Configuring trunks and channels” on page 5-14.

To better apply the general trunking concepts described in this chapter to your specific situation, refer to your Service Confirmation Letter and Trunk Provisioning Information Form from your service provider. For samples of these documents, see Appendix C.

Trunk and channel terminology

Before reading more about Wave trunks, you should understand how we use the following terms in the documentation and user interface.

- **Channel**. A path of communication between two points, typically between the phone company central office (CO), your service provider, and you, the subscriber. In Wave, a channel carries one voice call or one data connection.
- **Trunk**. The transmission media by which the central office or your service provider sends your phone and data signals, typically over cabling that plugs into various Wave hardware components.

    - **Analog trunk**. Transport a single channel of traffic and are commonly referred to as Plain Old Telephone Service (POTS) trunks (and sometimes known as *analog lines* or *analog channels*). These trunks are similar to the phone lines running into your house.

      In Wave terminology, we refer to analog trunks as either *trunks* or *channels* in the documentation, and as *channels* in the Management Console user interface.
    - **Digital trunk**. Transport multiple channels of traffic. Each *digital channel* can carry a single voice call or up to 1.544 Megabits per second (Mbps) of data traffic.
- **Line**. See *Channel*, above. Typically refers to analog, not digital channel.
- **Trunk group**. Indicates a grouping of analog or digital channels. These groupings can handle inbound calls, outbound calls, or both, depending on the trunk group or connection type, and they can handle *only* voice traffic.
- **Connection**. A Wave term used to indicate a grouping of digital channels configured to handle network traffic. These groupings can handle *only* data traffic.
- **Card or module**. A Wave hardware component into which the cables carrying the signals from the central office (your trunks) plug.
- **Port**. The physical receptacles, one per trunk, on a card or module into which cables plug.

Some terms are used differently when referring to analog vs. digital media. The following table describes these differences (*card*, *module*, and *port* are not included in the table, because these terms are identical across analog and digital media.)

Term	Analog	Digital
Channel	A single call; same as *trunk* and *line*	A single call or data connection
Trunk	A single channel, call; same as *channel* and *line*	Multiple channels carrying multiple calls or data connections
Trunk group	A named, specified group of voice channels, or trunks	A named, specified group of voice channels
Connection	N/A	A named, specified group of data channels

Analog and digital trunks

Wave supports both analog and digital trunks. Your central office provisions each of your trunks for specific handshake and signaling options, which they provide in your Service Confirmation Letter. (See Appendix C for an example.) You must enter these values in Wave for the trunks to operate properly with the equipment on the service-provider end of each trunk.

Before you configure trunks, ensure that your trunk groups are configured appropriately. For more information about trunk groups, see “Trunk groups” on page 27-4. For trunk group configuration procedures, see “About creating new trunk groups” on page 5-2.

Analog trunks

The Integrated Services Card in your Wave Server provides 4 analog trunk ports. Additional analog trunk ports may be available if one or more modules that provide analog trunk ports (Analog Trunk Module or Analog Universal Module) are installed on your Wave Server. Each trunk can carry a single voice call or a single 56 Kbps modem data call.

Note: The Wave Server supports one 56 Kb modem call using the internal modem on the Integrated Services Card. You can connect additional modems externally to analog station ports.

For trunk configuration procedures, see “Configuring trunks and channels” on page 5-14

Digital trunks

The Wave Server supports the following digital connections:

- **T-1**. Transports a stream of Digital Signal 1 (DS1) frames. Each frame transports up to 24 channels of traffic, with each channel supporting a single voice call or 56/64 kilobits (Kb) of data traffic. You can configure each of the 24 channels of the T-1 connection independently to transmit voice or data.

  The Wave Server supports data connections up to 1.544 Megabits per second (Mbps) and can switch voice and data traffic from four T-1 connections simultaneously.

  For T-1 configuration procedures, see “Configuring digital trunks and channels” on page 5-22.

In addition, the T-1 card incorporates a T-1/DS0 Multiplexor, also known as the DS0 Digital Access Cross-Connect Switch, that provides the capability**—in software and without additional hardware—**to individually cross-connect DS0s (a single channel) from one digital interface to another, allowing DS0s to pass through the Wave without terminating on an internal device. To do this, you assign the T-1/DS0 Mux connection to the channels you want to cross-connect to another T-1 interface. You connect one of your T-1 ports to your incoming T-1 connection and another T-1 port to the external device (for example, another router).

For DS0 Mux configuration procedures, see “Configuring digital trunks and channels” on page 5-22.

- **ISDN PRI**. Transports data at 1.544 Megabits per second (Mbps). The Wave Server supports ISDN PRI on any or all of the digital trunks on T-1. This includes support for Network Service Facility (NSF) codes for least cost routing on a call-by-call basis over an ISDN PRI trunk (if your trunk supports multiple services). Each of the 24 PRI bearer channels (B-channels) can support a single voice or data call.

  You can specify the ISDN Type of Number (TON) and Numbering Plan Identifier (NPI) to enable connections to operate on different ISDN networks. When using ISDN PRI for a connection, you reduce the available channels by one per circuit.

  For ISDN configuration procedures, see “Configuring digital channels for ISDN” on page 5-35.

Trunk groups

By assigning analog or digital trunks to trunk groups, you enable the voice paths to the PBX subsystems of Wave. By assigning digital channels to data connections, you enable data paths to the network subsystems of Wave.

Before you work with analog or digital trunks on Wave, you might need to configure groupings of them. For trunk group configuration procedures, see “About creating new trunk groups” on page 5-2.

Voice and data traffic

Digital trunk groups can handle either voice or data traffic, and analog trunk groups can handle voice traffic.

- **Voice.** Analog or digital trunk groups configured for voice traffic direct inbound calls to a specific extension (station, hunt group, modem, or fax machine) and direct outbound calls from an extension to an available trunk of the trunk group.
- **Data.** Digital connections bind WAN data traffic to and from the Wave LAN segment(s) and direct data signals traveling via channels directly to logical router interfaces of the Microsoft Routing and Remote Access Service (RRAS). This is how Local Area Network (LAN) traffic is passed to and received from the connection.

  You can use the following connections to transport data between the Wave Server and the WAN:

  - DS0/Mux
  - Serial, which enables you to cross-connect digital channels to a serial interface to an external router

Wave default trunk groups and connections

Wave provides default groupings that you can use to quickly group a set of analog or digital channels.

Default trunk groups

The following table describes the default analog and digital trunk groups, which appear in the Trunk Groups applet.

Default Group	Description
Voice Analog	Configured to direct incoming analog voice traffic to a default destination (attendant, extension 0).
Voice Digital	Not configured. A named, placeholder trunk group for you to configure.
DID Analog	Not configured. A named, placeholder trunk group for you to configure.

Default Group	Description
DID Digital	Not configured. A named, placeholder trunk group for you to configure.
Modems	Configured to direct data traffic traveling on either digital channels or analog trunks to an internal 56 Kbps modem in the Wave Server (hunt group 570). This group routes data traffic for dial-up or dial-in computer client connections. The channel or trunk assigned to the Modem group should be dedicated lines (phone numbers). Calls directed by the Modem group are sent to extension 570 (the default modem hunt group).

In most call routing scenarios you do not need to create additional groups—the defaults should provide you with the functionality that you need.

You might need to create new trunk groups, however, to handle multiple-trunk call-termination scenarios. If so, you need all of the trunk information available from your service provider, for example:

- The range of DID numbers
- Whether the DID T-1 channels and analog trunks are inbound or bidirectional (2-way)
- How many digits are they sending (usually 3 or 4)

If your call scenario requires additional groups, see “About creating new trunk groups” on page 5-2.

Default data connection

The following table describes the default data connection, which appears in the Trunk Configuration applet.

Default Connection	Description
T-1/DS0 Mux	Configured to provide the capability—in software and without additional hardware—to individually cross-connect DS0s from one digital interface to another, allowing DS0s to pass through the Wave without terminating on an internal device.

Trunk group hunt types

When users make outbound calls on Wave, the hunt type of the associated trunk group determines how an available analog trunk or digital channel is located. Trunk groups can hunt in either a linear or a circular fashion and either of those hunt types can be used in forward or reverse order.

- **Linear.** Looks for a free channel, always starting at the beginning of the list of trunk groups and searching to the end, or—for reverse-order hunting—always starting at the end of the list and searching to the beginning. Each channel is tried once.
- **Circular.** Looks for a free channel, starting where the last search left off. From this point (where the last search left off), forward-order hunting works forward through the list of available channels, and reverse-order hunting works backward through the list. Each channel is tried once.

When you configure trunk groups, you will set the hunt type for each. For trunk group configuration procedures, see “About creating new trunk groups” on page 5-2.

Minimizing Glare

Glare occurs when an incoming call and an outgoing call select the same channel simultaneously. For example, GlareGlobalAdministrator occurs when Wave receives a call from the network on a channel it has just selected to initiate an outbound call. In this case, Wave allows the inbound call to use that channel and retries the outbound call on a different channel.

Reverse-order hunting helps reduce collisions with the central office’s incall hunt group. The central office will typically use incall hunt groups that are linear and start with the lowest trunk or channel.

To minimize Glare:

1. Determine the central office (network side of the connection) hunt order.
2. Configure Wave (user side of the connection) for the opposite hunt order.

   For example, if the central office is configured for linear hunting, configure Wave for reverse linear hunting.

Note: When connecting two Wave Servers together using ISDN, set the network side of the connection to the linear hunt type and the user side to the reverse linear hunt type.

Hunt type examples

Assume channels 1 through 5 belong to the same outbound trunk group.

Forward-order linear searching

- Request for external line: accepted by outbound connection
- Check digital channel, channel 1: busy
- Check digital channel, channel 2: busy
- Check digital channel, channel 3: available—call placed
- Request for external line: accepted by outbound connection
- Check digital channel, channel 1: busy
- Check digital channel, channel 2: available—call placed

In this example, each time a request for an external line is made (typically by the user dialing 9 to access an external line) the trunk group members (individual digital channels) are searched in order.

Reverse-order linear searching

- Request for external line: accepted by outbound trunk group
- Check digital channel, channel5: busy
- Check digital channel, channel 4: busy
- Check digital channel, channel 3: available—call placed
- Request for external line: accepted by outbound trunk group
- Check digital channel, channel 5: busy
- Check digital channel, channel 4: available—call placed

Forward-order circular searching

- Request for external line: accepted by outbound trunk group
- Check digital channel, channel 1: busy
- Check digital channel, channel 2: busy
- Check digital channel, channel 3: available—call placed
- Request for external line: accepted by outbound trunk group
- Check digital channel, channel 4: busy
- Check digital channel, channel 5: available—call placed
- Request for external line: accepted by outbound trunk group
- Check digital channel, channel 1: busy
- Check digital channel, channel 2: available—call placed

Reverse-order circular searching

- Request for external line: accepted by outbound trunk group
- Check digital channel, channel 5: busy
- Check digital channel, channel 4: available—call placed
- Request for external line: accepted by outbound trunk group
- Check digital channel, channel 3: busy
- Check digital channel, channel 2: busy
- Check digital channel, channel 1: available—call placed
- Request for external line: accepted by outbound trunk group
- Check digital channel, channel 5: busy
- Check digital channel, channel 4: available—call placed

Chapter 28

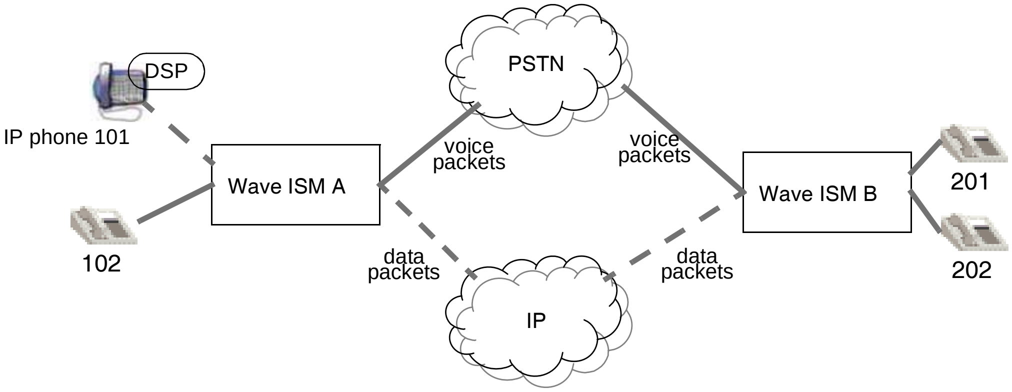
Understanding Wave IP Telephony

CHAPTER CONTENTS

This chapter describes how IP telephony is implemented in Wave, and how you can use Wave ISM to route voice calls over your data network.

What is IP telephony?

IP telephony, also known as voice over IP, allows you to make phone calls using segments of your data network rather than the traditional Public Switched Telephone Network (PSTN). The two different types of calls are transmitted over different networks, as shown in the following illustration:



To transmit voice over the data network, a Digital Signal Processor (DSP), using a codec (a signal compression-decompression algorithm), splits up the voice signals into small parts, compresses them, and inserts them into data packets. The packets are addressed to the call recipient (an IP address) and sent out over the data network. The packets are reassembled by a DSP at the receiving end.

Using IP telephony, Wave users can:

- Call extensions on remote Wave sites over the data network (site-to-site IP calls)
- Save money on long distance calls by using a virtual tie-line to place calls through a remote Wave system (sometimes called tandem call routing).
- Accommodate remote workers and small satellite offices with IP phones (telecommuters, small branch offices)

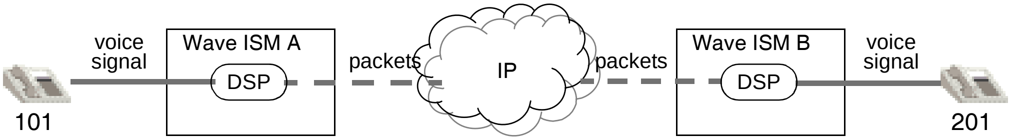
IP call scenarios supported on the Wave system

An IP call is a phone call in which at least one portion of the voice signals are transported across a data network. Wave ISM supports the following IP call scenarios:

- Site-to-site IP calls
- IP phone calls

Site-to-site IP calls

A site-to-site IP call is a phone call in which the segment of the call path between two Wave Servers is on the data network, as shown in the following illustration:



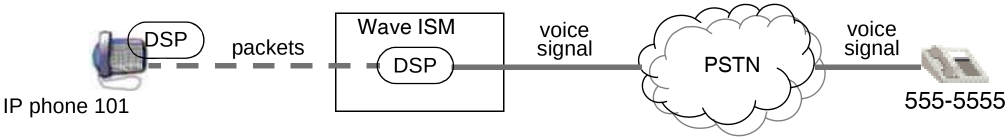
For more information about the DSPs, licenses, and configuration required for this scenario, see the following sections of this document:

- “DSP resources required in a site-to-site scenario” on page 28-5
- “Direct site-to-site IP calls” on page 28-8

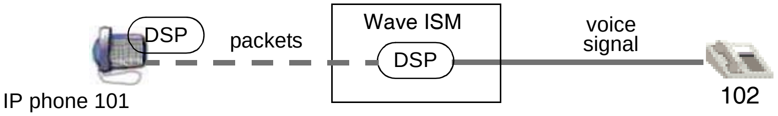
IP phone calls

An IP phone is connected directly to the data network; therefore, a call involving an IP phone uses the portion of the data network between the IP phone and the Wave system. IP phones can make calls to devices on the PSTN, to internal analog and digital phones connected to the Wave Server, and to other IP phones.

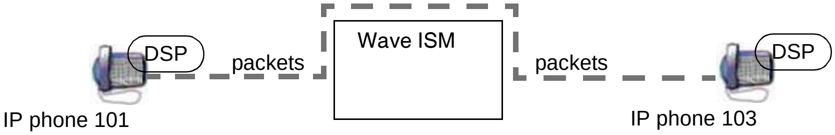
The following illustration shows an IP phone call to a device on the PSTN:



The following illustration shows an IP phone call to a phone connected to the Wave Server:



The following illustration shows an IP phone call to another IP phone:



For more information about the DSPs, licenses, and configuration required for these scenarios, see the following sections of this document:

- “DSP resources required in scenarios with IP phones” on page 28-6
- “IP phones” on page 28-8

DSP resources and licensing for IP telephony resources

Digital Signal Processor (DSP) resources applied to IP telephony give the Wave Server the capability to route voice calls over packet-switched (data) networks. DSPs can convert voice signals into data packets, and vice versa, using a codec.

The number of DSP resources you have available for IP telephony on your Wave Server depends upon the hardware installed on your system and the IP Gateway licenses that you purchase.

How many DSPs do you need?

The more DSPs you allocate to IP telephony in the Resource Management configuration, the more concurrent IP calls your system can support. To estimate the number of DSPs you require at each site, remember that each time a transition is made between TDM voice signals and packets in the voice path, a DSP is required to make the conversion.

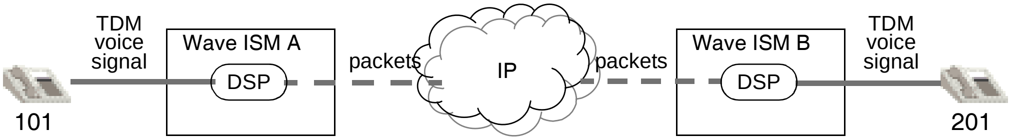
Note: Calls between IP phones do not require any DSPs on the Wave Server.

Most IP calls will require two DSPs, one at each end of the IP segment of the call. The DSPs may be located on the Wave Server, or they may be located on the IP phones, depending on the calling scenario.

Important! Additional DSP resources are used only briefly during the life a of a call or while a feature is being used. You must allocate these additional DSP resources manually. See “Resource requirements for transitory events” on page 23-44 for more information.

DSP resources required in a site-to-site scenario

The following illustration shows the DSPs required in a direct site-to-site IP call scenario over a packet-switched network segment. (See “Direct site-to-site IP calls” on page 28-8 for a detailed explanation of this scenario). In this scenario, the phones are traditional TDM calling devices (the analog or digital phones).



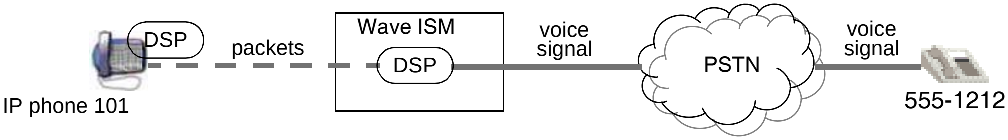
A DSP on Wave Server A translates the voice signal (from the caller at extension 101) into packets that can be sent over the IP network. The receiving Wave Server B uses a DSP to translate the packets back into a voice signal that can be understood by the call recipient at extension 201, and vice versa. If you want to support four calls of this type at once, each Wave Server would require four IP telephony DSP resources.

DSP resources required in scenarios with IP phones

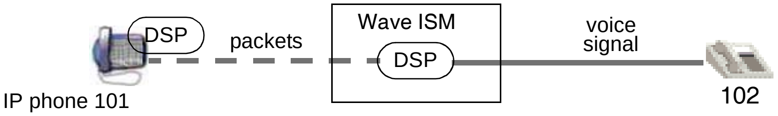
The DSPs required for phone calls involving IP phones may vary depending on how many IP phones are involved in the call.

In the first two examples illustrated below, two DSPs are required for each call, but only one DSP is required on the Wave Server itself, since there is a DSP in the IP phone.

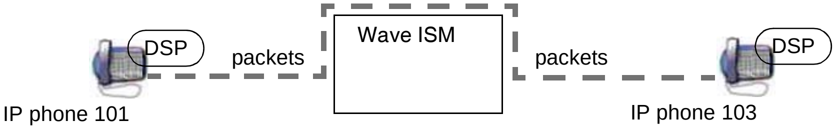
The following illustration shows an IP phone call to a device on the PSTN:



The following illustration shows an IP phone call to a phone connected to the Wave Server:



The following illustration shows the DSPs required to make a call between two IP phones on the Wave Server. Note that no IP telephony resources are required on the Wave system in this scenario.



Other DSP applications

DSP resources are also required by TAPI-based telephony applications, such as voicemail. Since TAPI applications and IP telephony cannot share the same DSP resource, you must distribute the DSP resources between TAPI applications and IP telephony based on your business requirements. See “Managing Wave system resources” on page 23-43 for more information.

IP call routing

Call routing for IP telephony is similar to traditional call routing. This section assumes that you are familiar with Wave call routing mechanisms. Chapter 29, “Understanding Wave Call Routing,” provides information about how calls are routed in the Wave system.

For IP call routing configuration procedures, see “Configuring site-to-site call routing for IP telephony” on page 6-4.

Signaling Control Points

A Signaling Control Point is an IP telephony endpoint that is capable of originating and terminating IP calls. A Signaling Control Point is defined by an IP address and an IP telephony signaling protocol. Its traditional Wave call routing counterpart is the trunk group.

Signaling Control Points can be substituted for trunk groups in any of your outbound call routing scenarios. For inbound call routing, each Signaling Control Point configuration includes an inbound call routing table where you can specify how to handle calls from each source.

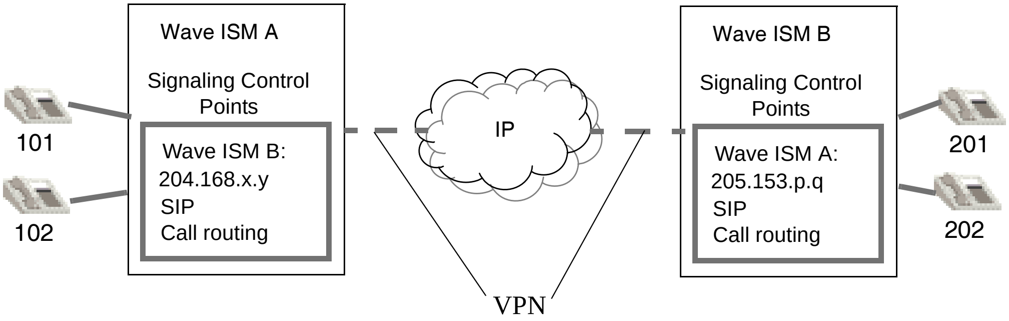
Each Signaling Control Point configuration includes the remote Wave Server’s IP address, signaling protocol, and call routing parameters. Once the Signaling Control Points are configured you can include them as call destinations in your outbound call routing configuration. See Chapter 29, “Understanding Wave Call Routing,” for information about Wave call routing.

Default inbound routing

To specify how to route incoming IP calls from unknown sources (that is, a call from an IP address that is not included in your Signaling Control Point configurations), configure the call handling rules with the default inbound call routing settings. Refer to “Configuring default inbound IP call routing” on page 6-26 for more information.

Direct site-to-site IP calls

Direct site-to-site calling requires that every Wave Server using IP telephony specifies a Signaling Control Point for every other IP telephony-enabled Wave Server on the network as shown in the following illustration. In this example, Wave Server A has a Signaling Control Point configured for Wave Server B, and vice versa.

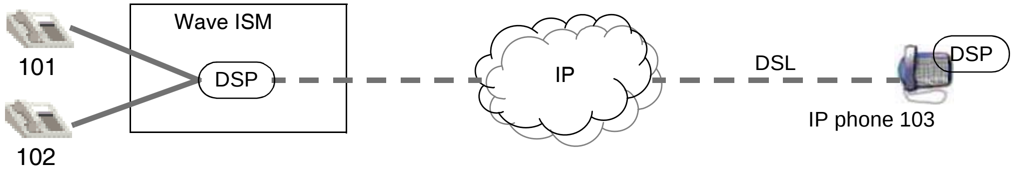


IP phones

IP phones are a convenient way to set up communications between a remote worker, such as a telecommuter, and the main office where a Wave Server is running. IP phones are also a cost effective alternative to setting up a PBX for a small satellite office with fewer than five users. IP phones in each of these scenarios can be set up at the remote site, and the IP call routing is controlled by the Wave Server at the main office.

Note: A remote IP phone will not work with a traditional firewall or Network Address Translation (NAT) router—you need to use a VPN connection.

The following illustration shows an IP phone for a remote worker or satellite office:



IP phones are configured much the same way as other Wave phones are configured in the User/Group Management applet. Each phone gets a primary extension number and can use a wide variety of PBX features on the Wave Server. The physical phone set also requires some configuration to initiate communication with the Wave Server. See "Configuring SIP phones" on page 6-29 for configuration procedures.

License requirements for IP phones

In order to use most IP phones with your Wave Server, you must purchase and enable IP User and IP Gateway licenses. (Vertical 5xxx IP phones come with the licenses included.) Contact your Vertical provider for more information.

MAC addresses

IP phones do not use station card ports like TDM phones; instead they connect over the data network, so the Wave ISM relies on the MAC address as the unique identifier for each IP phone.

Just as the Wave Server uses a station card slot number and port number to associate an extension configuration with a TDM phone, a MAC address is used to associate an extension configuration with an IP phone.

IP addresses

In addition to a MAC address, IP phones also need IP addresses for call routing purposes. IP addresses can be assigned to each phone by a DHCP server, or the phone can be configured with a static IP address.

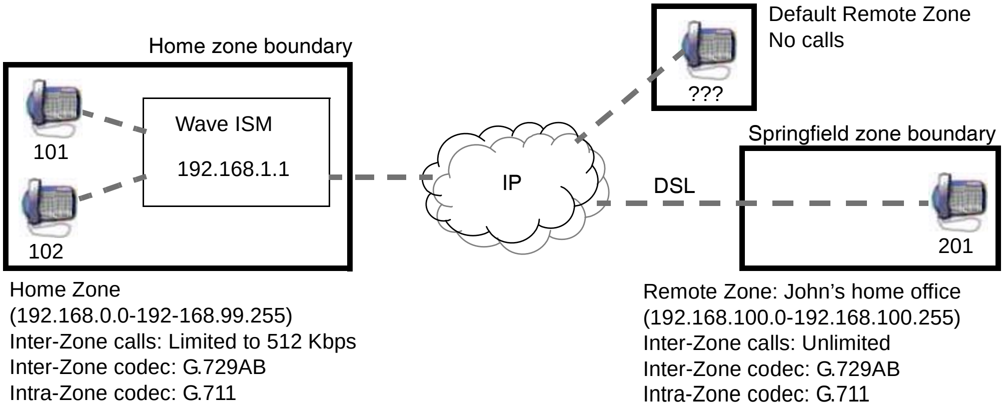
Bandwidth management

To manage bandwidth across different segments of the network you must create zones that define your network boundaries for IP telephony. Configuring bandwidth management zones allows you to control how much IP call traffic goes across different parts of your data network. It prevents your IP telephony users from making more IP calls than the network connections are capable of supporting.

A bandwidth management zone is defined by a range of IP addresses. You can create as many zones as you have boundaries where you need to control bandwidth use. There are three types of configurable zones:

- **Home Zone**. This is the zone that controls IP call bandwidth on your local Wave Server.
- **Remote Zone**. Remote zones control bandwidth usage on sets of IP address at a remote site, for example a branch office or home office.
- **Default Remote Zone**. This zone handles bandwidth management for IP calls from any IP address that is not defined in one of the other zones. A call from an undefined IP address is constrained by the properties configured in the default remote zone.

The following illustration shows bandwidth management zones:



The bandwidth management zone parameters you can configure include the maximum amount of bandwidth used for all calls across a zone boundary, and the preferred codecs, desired transmit packet times, and desired silence suppression setting for inter-zone and intra-zone IP calls.

Intra-zone calls are calls made between phones within a zone boundary. Inter-zone calls are calls that are made across zone boundaries. Codecs should be assigned such that you can maximize bandwidth on both inter-zone and intra-zone IP calls. Calls within a zone boundary are likely to have more bandwidth available to them than calls connected across zone boundaries.

IP call quality management

There are several advanced settings, in addition to the Bandwidth Management settings, that allow you to manage the quality of your IP calls.

- Jitter buffer
- Echo cancellation
- Comfort noise
- Gain
- DTMF transport settings
- Quality Of Service (QoS) settings

Caution! *These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative. Information about these settings is located in "Adjusting IP call quality parameters" on page 6-52.*

Chapter 29

Understanding Wave Call Routing

CHAPTER CONTENTS

This chapter contains information about the different types of call routing supported by Wave, and defines and describes the Wave ISM components used to route calls.

About call routing

There are two major steps in Wave call processing: digit collection and call routing. It is important to note that digit collection and call routing are two completely separate processes. In the digit collection process, the PBX collects the digits sent from the call source until it has enough digits to route the call. Once digit collection is complete, the PBX attempts to route the call.

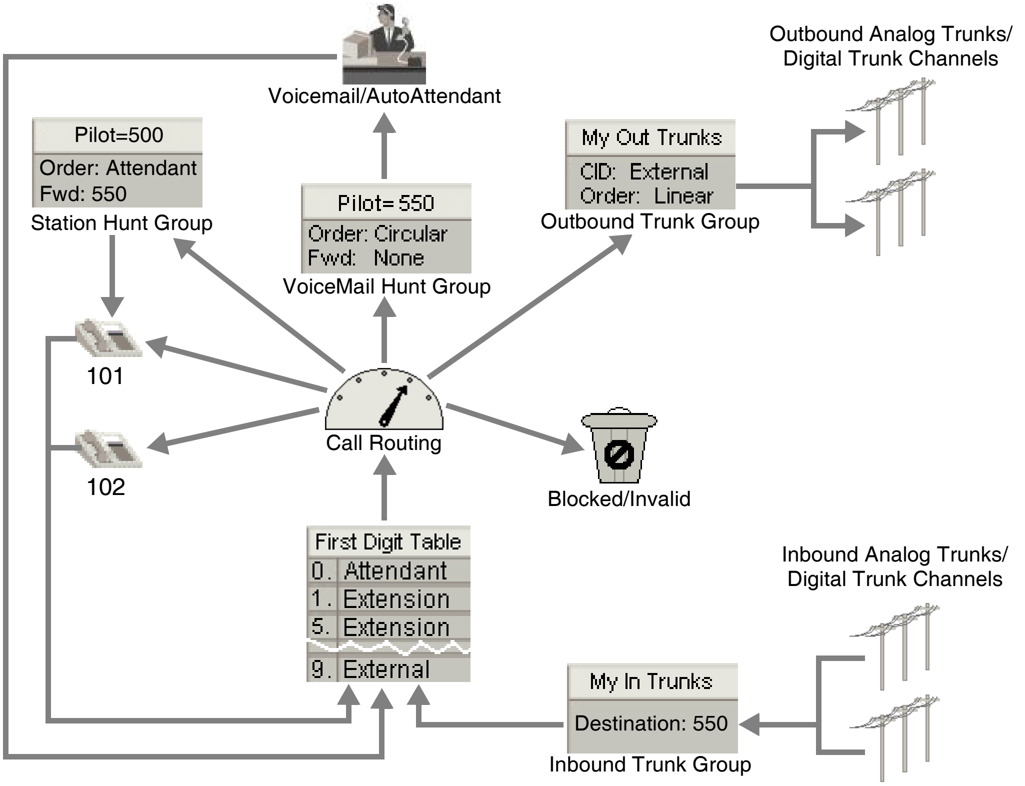
All calls that go through Wave pass through the First Digit Table. The first step in all Wave routing decisions is made based on the first digit of the number dialed. The first digit determines whether the call is routed to an internal or external destination.

When the destination is a user extension, the call is routed according to the user's active routing list.

A call route is a path through Wave by which a call goes from a source to a destination. There are four types of call routes to consider:

- **Internal**. From an internal source to an internal destination (usually extension to extension)
- **Outbound**. From an internal source to an external destination
- **Inbound**. From an external source to an internal destination
- **Tandem**. From an external source to an external source

Each section in this chapter describes and gives examples of each of the four call routing types. The following diagram provides a simplified view of Wave call routing, and all the major system components a call can pass through on its way to its destination, including the First Digit Table):



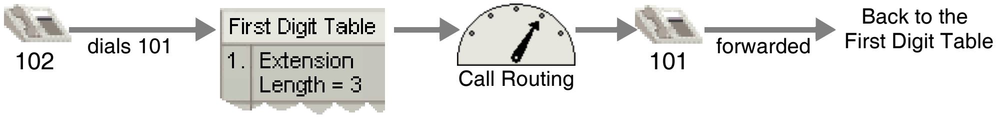
The following table describes the digit types contained in the first digit table:

First Digit Type	Description
Attendant	The Attendant digit serves two purposes: • If the caller dials (or transfers a call to) the Attendant digit from a phone connected to Wave, the PBX connects the caller to a member of the Attendant hunt group. • If the caller is connected to AutoAttendant and dials the Attendant digit, the caller is connected to the operator designated in the AutoAttendant schedule. Any digit (but only one) can be configured as the Attendant digit. The default is zero (0). If the Attendant digit is changed from the default of zero (0), the Attendant hunt group pilot number must also be changed, to ensure that the attendant will receive all calls routed to the attendant. **Caution:** *It is not recommended that you route inbound calls to zero because there can be no voice mailbox associated with this destination.*
Extension	The extension digit instructs the PBX to connect calls beginning with these digits to an extension number (or hunt group pilot number). The number of digits to collect following an extension digit is defined in the First Digit Table. The zero (0) digit cannot be configured for extensions. Default extensions begin with the digit 1 and 5, and are in the range 100-199 and 500-599. Hunt groups use extension numbers to pilot calls to the members of a hunt group. For example, Wave modems are preconfigured to be in hunt group 570.
External	An external digit at the beginning of a number instructs the PBX that an outbound, external call is beginning. You can define the external first digits (also known as destination access codes) as being one or two digits in length. Digit collection rules for numbers beginning with external digits are defined in the First Digit Table. The default external digit, 9, requires all users to press 9 on their phone dial pad before dialing any external number to be routed to the public switched telephone network (PSTN).
Not configured	A digit that is not configured instructs the PBX that calls beginning with these digits are not valid. If a user dials an unconfigured first digit, the PBX plays a fast busy tone to indicate that the first digit dialed is invalid.

Internal call routing

Internal call routing refers to all calls that originate and terminate within Wave. Internal calls can include calls such as station-to-station, station-to-hunt group, station-to-voicemail, and station-to-Attendant hunt group.

The following diagram shows how a station-to-station internal call flow might look:



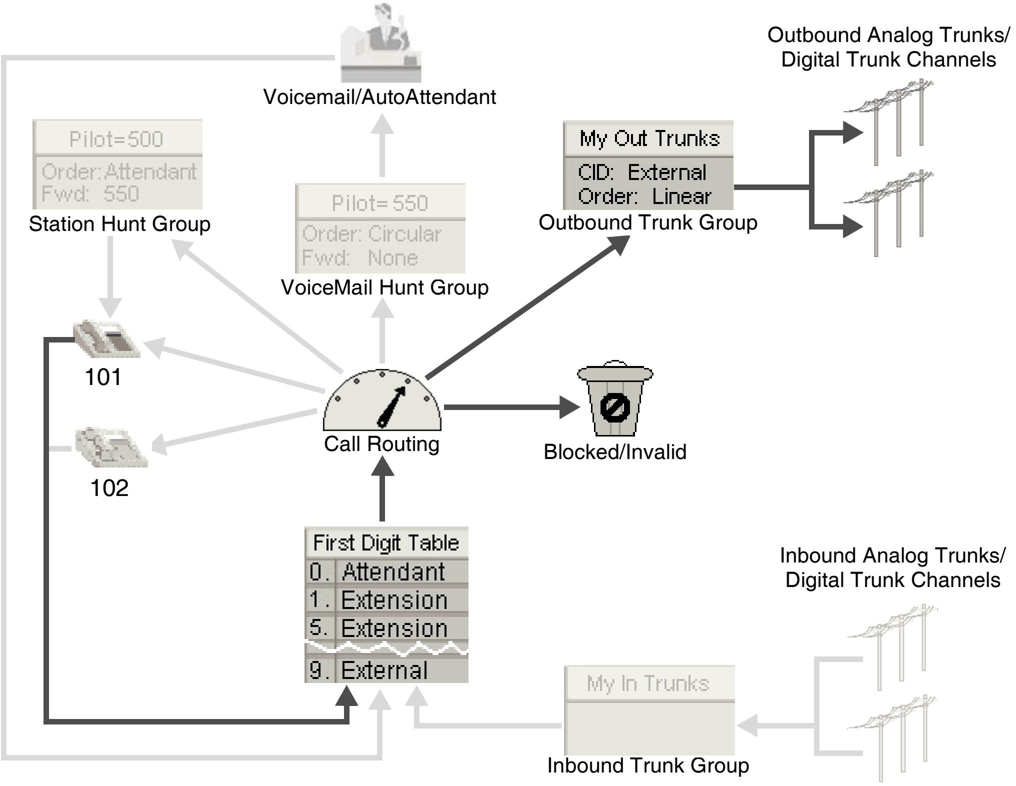
This diagram illustrates the following:

1. The user at extension 102 dials 1-0-1.
2. The first digit collected, 1, is specified in the First Digit Table as type Extension (and requires 2 additional digits to be collected before routing the call).
3. Once a three digit number beginning with 1 is collected, the PBX looks for extension 101.
4. Extension 101 exists, so the PBX routes the call to extension 101.
5. If the call to extension 101 is forwarded (or transferred), it goes through another round of call routing beginning with the First Digit Table. If extension 101 is a user (not a hunt group), the call is routed according to extension 101's active routing list.

Outbound call routing

Outbound call routing refers to calls that originate within Wave and terminate outside Wave (over a trunk connected to the Wave Server). These calls can include outbound calls from phone extensions, modems, and FAX machines.

The following diagram shows a simplified outbound call flow:



North American Numbering Plan

Wave collects digits using the North American Numbering Plan by default when processing calls using automatic route selection. The North American Numbering Plan requires phone numbers to have 10 digits and identifies them using the following numbering scheme:

- A three-digit area code
- A three-digit local exchange (or central office code)
- A four-digit subscriber number

If Wave sees a number (following the external digit) beginning with a number other than a 1, it is identified as a local (7-digit or 10-digit) number. (If the local area codes for 10-digit dialing are included in the First Digit Table, then there is no need to dial a one to send calls to numbers in those area codes.)

If Wave sees a number beginning with a 1, it expects to collect 10 more digits before routing the call. If the number begins with 011, Wave expects a variable number of digits, and will route the call after the dialing time-out expires (or the user presses #).

Access profiles

Access profiles control the types of outbound calls that can be placed from different sources in Wave, such as specific phones and trunks or channels. Using access profiles, calls can be routed or blocked based on rules you specify. Access profiles assigned to specific call sources can be overridden in the global access profile Special Digits Table and area code table.

For example, if a phone is assigned an access profile that limits calls made from that phone to internal extension numbers, and a user dials a number beginning with an external digit, such as 9, the call will be blocked (and the user will hear a fast-busy tone). However, if the Special Digits Table in the global access profile allows the number 911 to be routed to a trunk group, a call to 911 from the restricted phone will be routed.

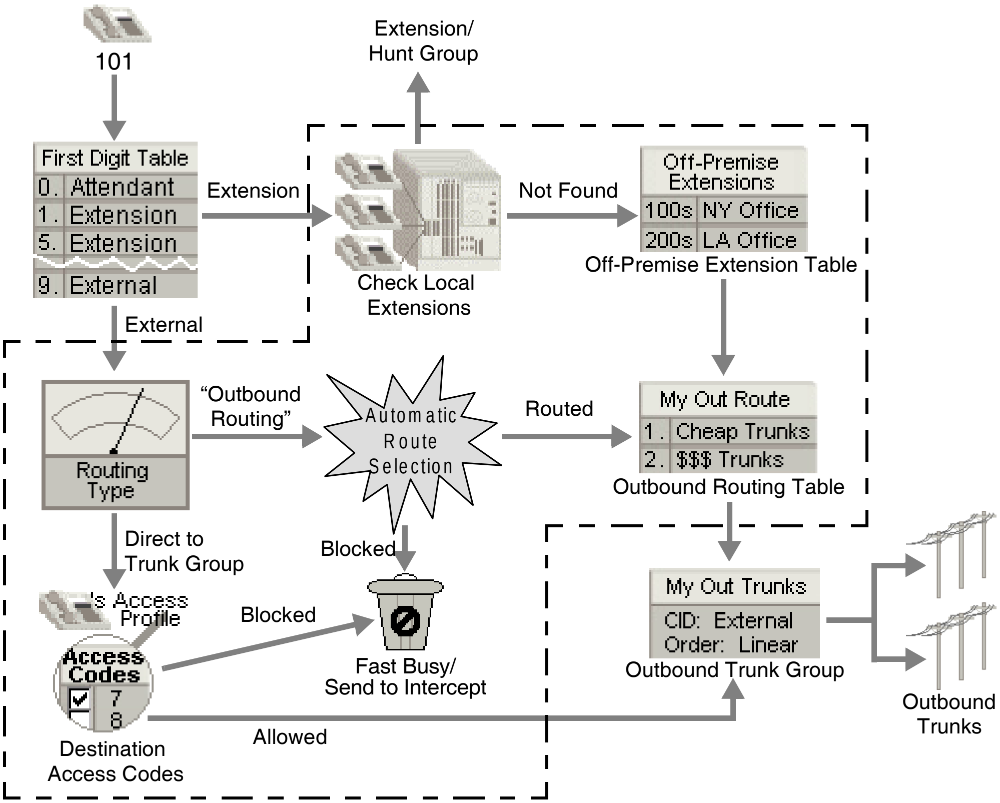
Outbound routing tables

Outbound routing tables are reusable, prioritized lists of outbound trunk groups (and IP telephony Signaling Control Points), and associated digit translation rules.

The routing tables allow you to set up outbound routing scenarios such as least cost routing, where Wave will first attempt to place a call over the cheaper trunk group. If the routing scenario fails, (because all the channels in that trunk group are in use, disabled, or disconnected,) the PBX attempts to place the call over the next trunk group specified in the next step in the routing table, and so on. (This is illustrated as My Out Route in the next diagram.)

An outbound routing table also allows you to translate the dialed number in a different way for each trunk group. For example, some trunks may require long distance numbers to be 10 digits, some 11 digits.

The following diagram illustrates the details of the outbound call routing process:



In this diagram, everything inside the dashed line represents the element labeled "Call Routing" in the simplified outbound call routing diagram on page 29-5. As you can see, there is more than one path an outbound call can take from the source to the trunk. Each path is described in detail in the following sections:

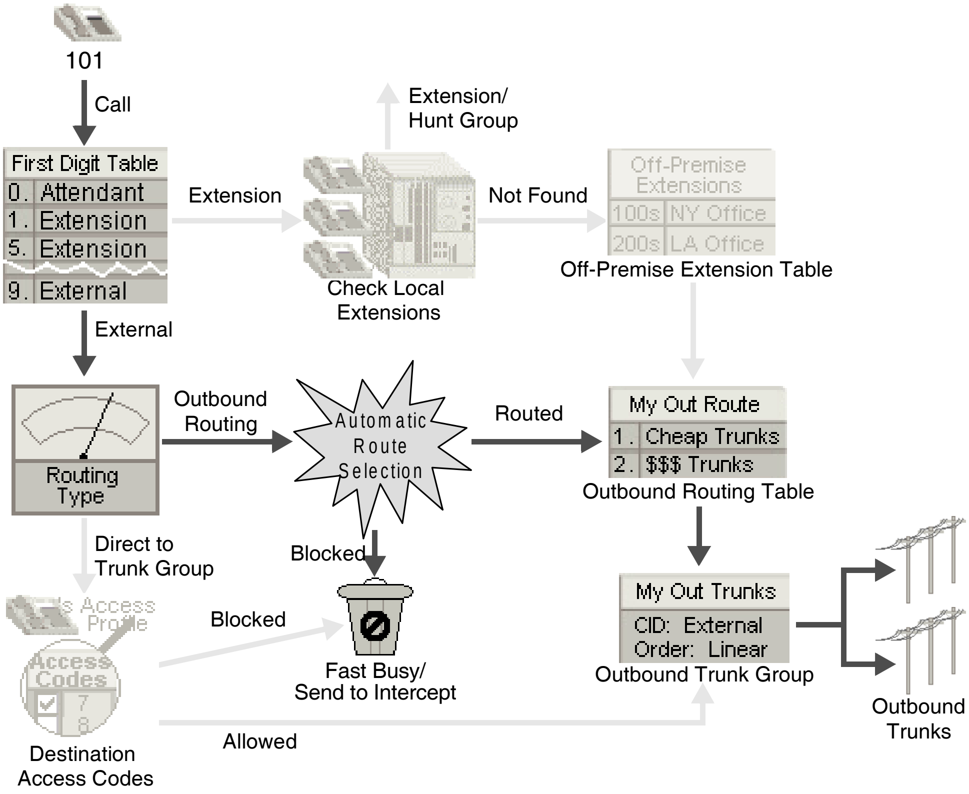
- Automatic route selection
- Off-premise extensions
- Destination access code/direct to trunk group

Automatic route selection

You use automatic route selection to route calls that connect to the central office. Automatic route selection is ideal when you want different types of outbound calls (local, long distance, toll free, international, etc.) to use different trunks. Automatic route selection allows you to:

- Restrict outbound calls based on call type or caller's privileges
- Select a trunk based on call type (least cost routing)
- Manipulate digits sent to the central office

The following diagram illustrates a simplified automatic route selection path:



The above figure shows the path by which a call is sent through Wave using automatic route selection. After determining that the call is an external call (based on the first digit collected), Wave looks up the routing type configured in the First Digit Table. In order to process a call using automatic route selection, the routing type must be **Outbound Routing**. Then the call is passed to the Automatic Route Selection process (detailed in the illustration on page 29-11 as all of the components contained within the dashed line.)

Special Digits Table

The Automatic Route Selection process first compares the dialed digits to the numbers in the Special Digits Table, which lists numbers that every phone in Wave is permitted to call (such as 911). In the Special Digits Table, numbers can be blocked, redirected to an internal destination, or routed to an outbound routing table. If a number does not have a match in the Special Digits Table, Wave determines the call type, and sends the call to the next appropriate routing step.

For example, if the number 555-1212 is dialed, it would find no match in the Special Digits Table. Since this is a 7-digit number, Wave uses the North American Numbering Plan to determine that this is a local call, and sends the call to the next step in the process.

Home area code

When 7-digit numbers are sent to the automatic route selection process, Wave looks up the home area code and sends this information along with the dialed number to the global area code table for further routing attempts.

In our example, Wave looks up the home area code (408), and sends this information along with the dialed number to the next step in the process.

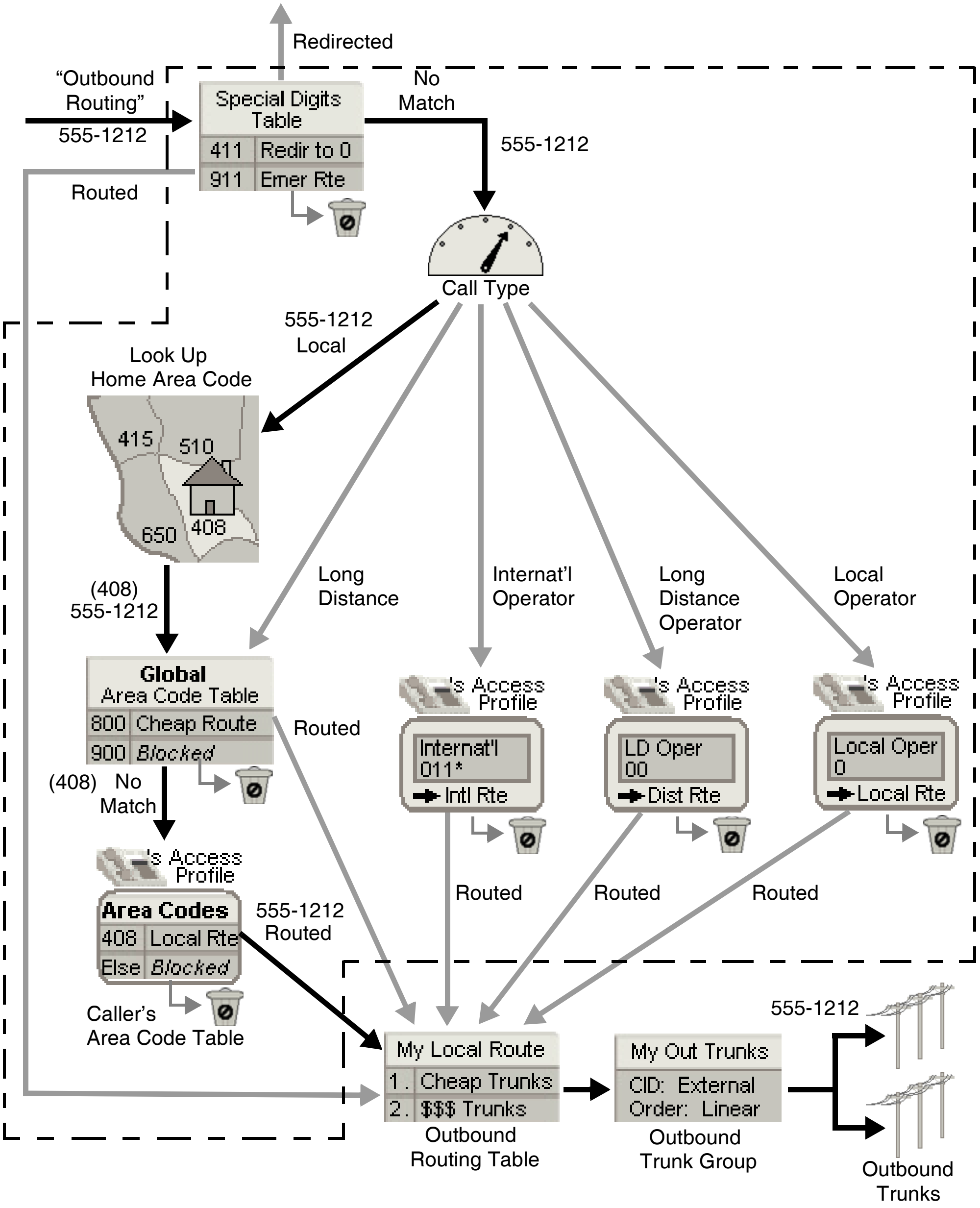
Area code tables

Dialed numbers are compared with the steps in the global area code table to find a match. Dialed numbers are first compared with area codes, then local exchange codes. If there is a match in the table for either code, the call is processed as instructed in the table (blocked or routed to an outbound routing table).

If there is no match in the global area code table, the dialed number is compared to the area code table assigned to the call source. If there is a match in this table, the call is processed (blocked or routed to an outbound routing table). Specific area codes tables should contain a rule that handles unmatched calls; blocking or routing them.

In our example, the area code, 408, is compared to the global area code table. Since neither the area code (408) nor the local exchange code (555) are in this table, the number is compared to the caller’s specific access profile area code table, where the area code is matched and the accompanying instructions indicate that the call should use My Local Route.

The following diagram illustrates automatic route selection detail showing a local call:



Long distance calls

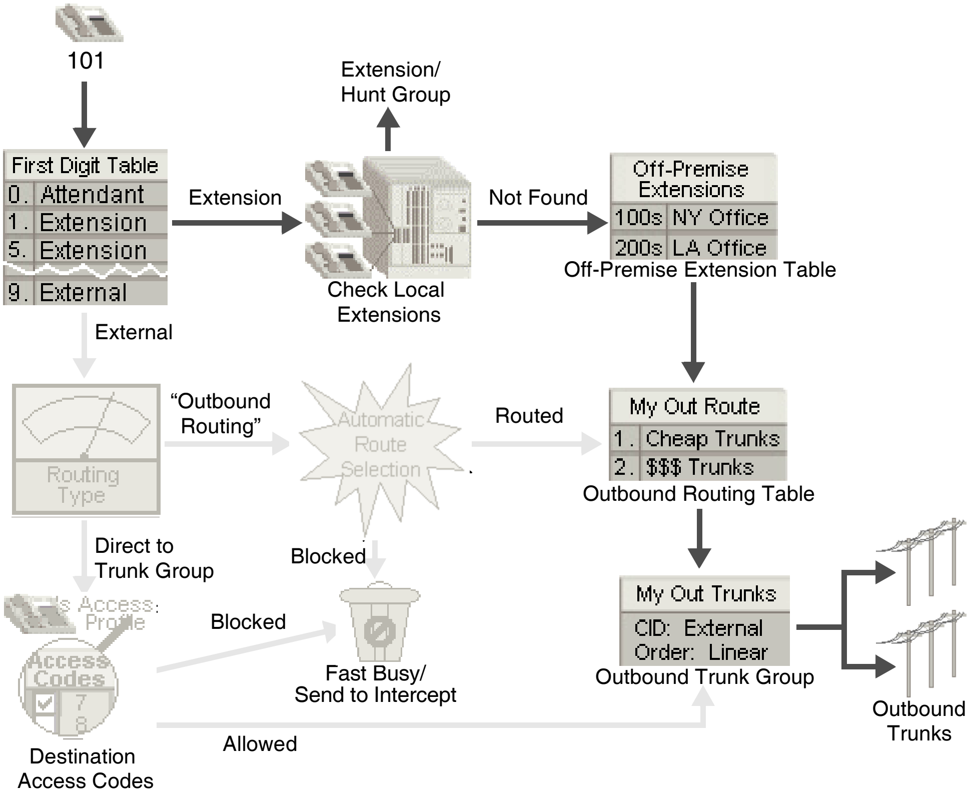
When long distance calls are processed using automatic route selection, the process is identical to the local call process, except that Wave skips the step of looking up the home area code.

Operator calls

Calls to international, long distance, or local operators, can be restricted (or routed) in the call source’s specific access profile.

Off-premise extensions

The following diagram illustrates an off-premise extension path:



Off-premise extensions allow you to route calls to extensions on other PBXs by dialing extension numbers.

The above figure shows the path by which a call to an off-premise extension is sent through Wave. After determining that the call is an internal one (based on the first digit collected), Wave looks up the local extension numbers.

If the extension number is not configured on the local Wave Server, Wave checks the off-premise extension table for the number. If the number exists in the table, the call is routed (or blocked). If the number does not exist in the table, the call fails and the user hears a fast busy tone.

Off-Premise extension table

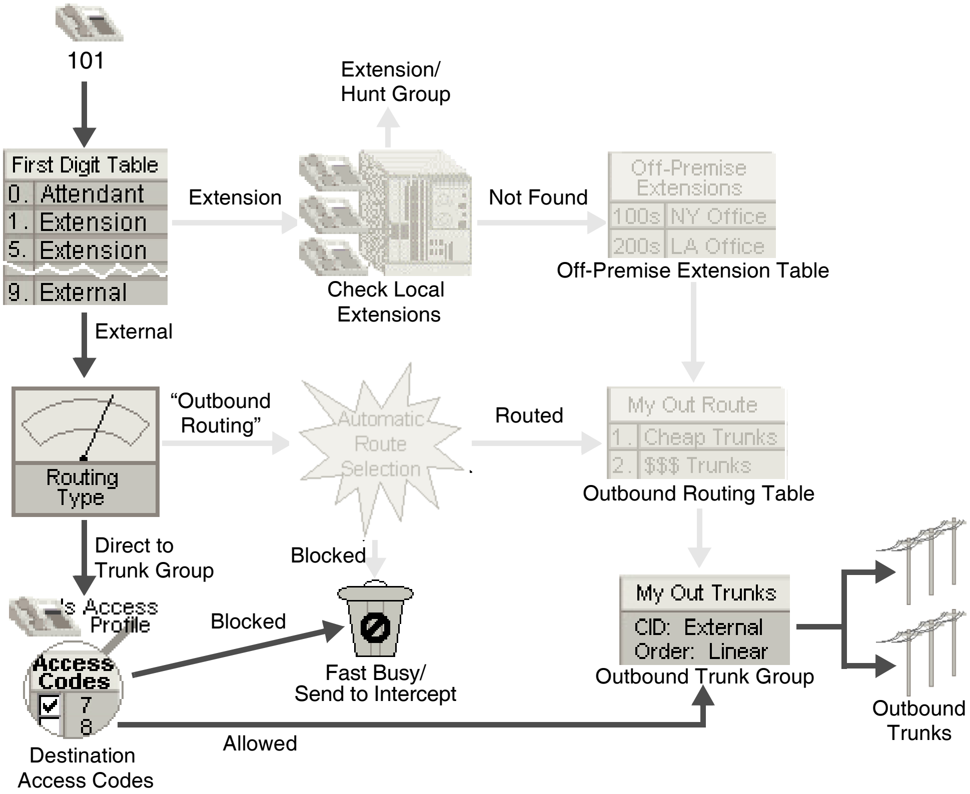
The off-premise extension table contains the ranges of extensions that exist on other PBXs (the range can include internal numbers). An outbound routing table is used to translate the number dialed and route the call to the trunk that will send it to the appropriate off-premise phone (see “Outbound routing tables” on page 29-6). In the outbound routing table you can translate the extension number to the appropriate number that will ring the extension on the far end.

Destination access code/direct to trunk group

Use destination access code/direct to trunk group routing to connect to another PBX that will handle dialing restriction and digit translation. Destination access codes restrict calls per user, not per call type, and do not allow you to do any digit translation, blocking, or alternate routing based on the dialed number. All callers using a particular access code use the same trunk group and are allowed to dial any number on the PSTN.

It is very important that you set the digit collection rules for each destination access code properly in the First Digit Table (see “Creating destination access codes” on page 9-26). Collecting too many or too few digits will cause calls using the access codes to fail. Using the call numbering plan (North American Numbering Plan by default) can help you avoid problems with calls bound for the PSTN.

The following diagram shows a simplified outbound call routing scenario highlighting destination access code/direct to trunk group routing:

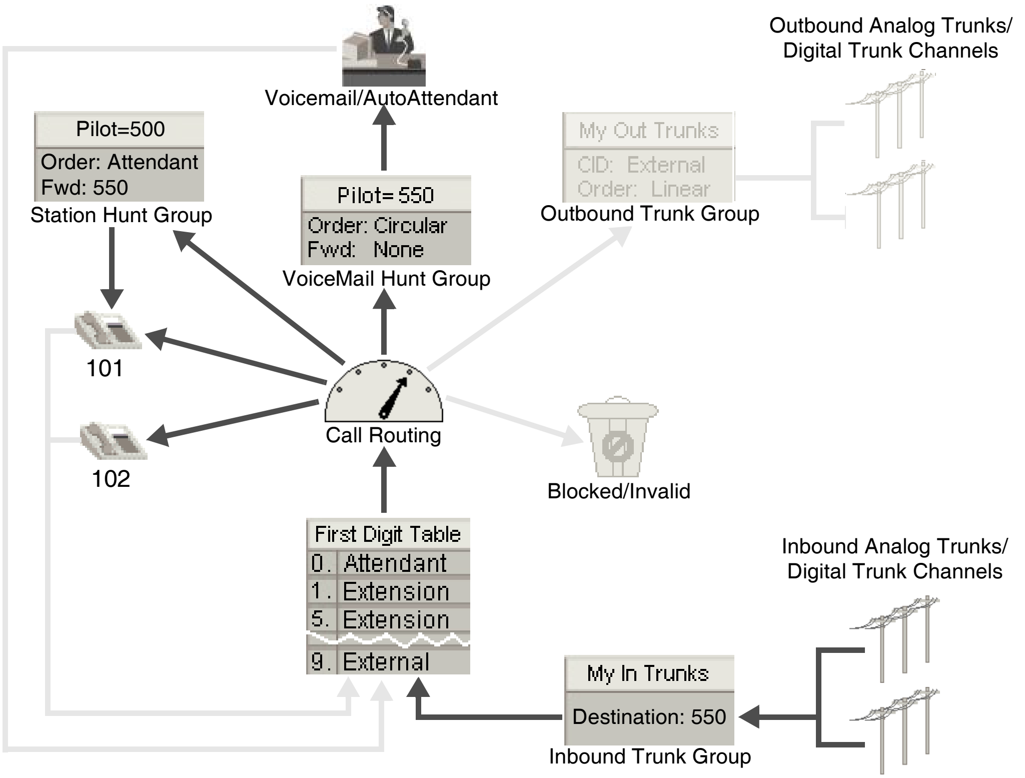


Destination access code table

A destination access code table allows Wave to verify that a specific extension has permission to use a destination access code (see Destination Access Codes in the figure above). Permission to use a destination access code is enabled in each of the destination access code tables associated with a specific access profile. Once an extension has permission to use the destination access code, the only restriction to the types of calls that can be made are the number of digits you collect.

Inbound call routing

The following diagram illustrates the simple inbound call path from the inbound trunks to the extensions and voice applications.



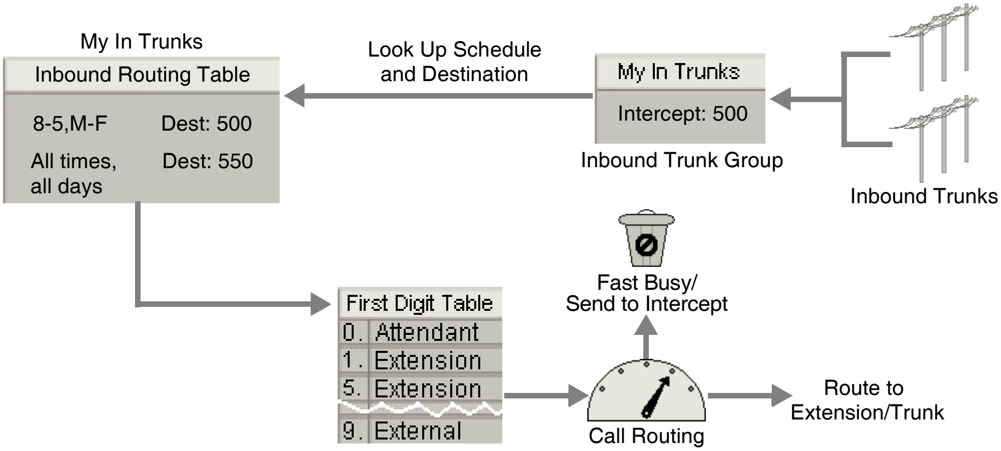
Inbound call routing must be configured differently depending on how the trunks are provisioned and what call information you receive from the far end (central office or another PBX). The digit collection and translation detail, between receiving calls on the trunks and routing those calls, is explained in each of the following sections:

- Trunks receive no digits
- Wink start DID trunks
- ISDN trunks
- Trunks receive digits from another PBX

Trunks receive no digits

When you configure inbound routing on trunks that receive no digits (usually analog trunks used for calls to the company main phone number), you will either route all calls on these trunks to a single destination, or route calls to different destinations based on a schedule. To accomplish this, use an inbound routing table with the Scheduled Routing option.

The following diagram shows scheduled routing inbound call routing details:



Inbound routing table

An inbound routing table is a prioritized list of digit- and schedule-matching translation rules for calls received on a particular trunk group. Inbound routing can be based on any of the following:

- Dialed number (, DNIS, Lead TN)
- Calling party number (Caller ID, ANI)
- Time of day and day of week
- All of the above

Inbound routing tables interpret digits collected from trunks, and translate them to numbers that can be interpreted by the First Digit Table. After receiving digits from the central office, the PBX searches the inbound routing table for the *first* matching step.

If a match is found, the call will be translated and sent to the corresponding destination number listed in the table. Then the First Digit Table uses the information to determine the call type and start the call routing process. If there is no match in the table, the call cannot be routed and is sent to the intercept destination specified in the inbound trunk group configuration.

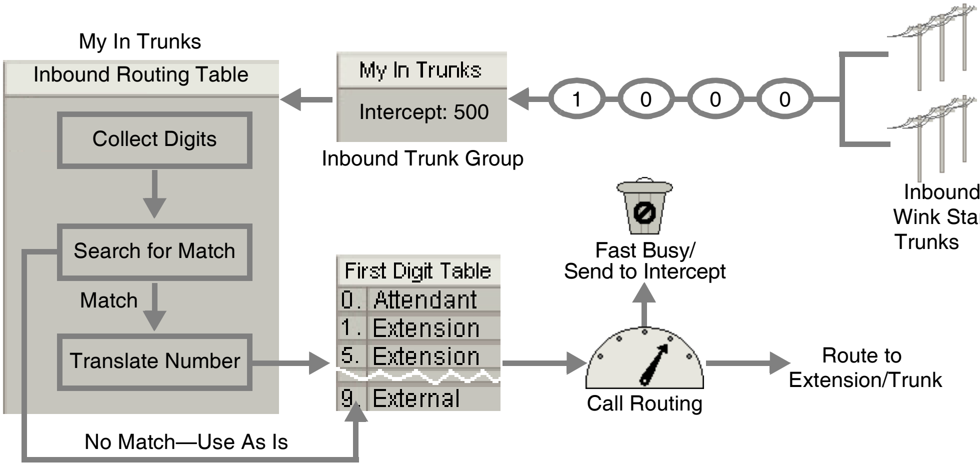
Observe the order that the steps appear in the inbound routing table in the previous illustration. The first and second step overlap, in the days of the week and times of the day they cover. The first step overrides the second step during the overlap.

In this example, the first step is configured to route calls to a live operator during normal business hours. The second step is configured to route calls to the AutoAttendant during non-business hours. The first step overrides the second step between the hours of 8:00 A.M. and 5:00 P.M., Monday through Friday.

Wink start DID trunks

Wink start DID trunks receive digits from the central office, which are used to route calls to various destinations in Wave. Since this type of trunk receives digits, you will want to use an inbound routing table that specifies digit collection rules.

The following diagram illustrates Wink Start DID inbound call routing details:



Digit collection

On wink start DID trunks you will receive digits from the central office one at a time as shown above the previous diagram. Wave keeps collecting digits until the number of digits collected matches the number of digits in the longest Dialed Number value in the inbound routing table.

The following table illustrates a sample inbound routing table:

Step	Dialed Number	Destination	Description
1	1000	550	AutoAttendant
2	1xxx	2xxx	Extensions (2001-2075)

For example, if the inbound routing table has two values for Dialed Number, Wave will wait to collect four digits. If Wave receives more than four digits, only the first four digits are considered and the rest are ignored. If Wave only receives three digits, the digit collection times out after a period, and Wave attempts to place the call with the digits it received.

Digit translation

The collected digits are compared with the steps in the inbound routing table. You can specify a destination that uses digits in the dialed number by using x's in the destination number. For example, if the dialed number is 1011, and the destination for numbers matching 1xxx is 2xxx, then the call is sent to extension 2011.

It is very important to place the steps in the order they must be considered by Wave. For example, if Wave has an inbound routing table that contains two steps, and it receives the digits 1-0-0-0, the first step is matched and the second step is not considered.

If you reverse the steps in , the call would not go to the AutoAttendant (550). Instead, Wave would attempt to locate extension 2000, which does not exist, and the call fails (or is routed to the intercept destination, if one is configured).

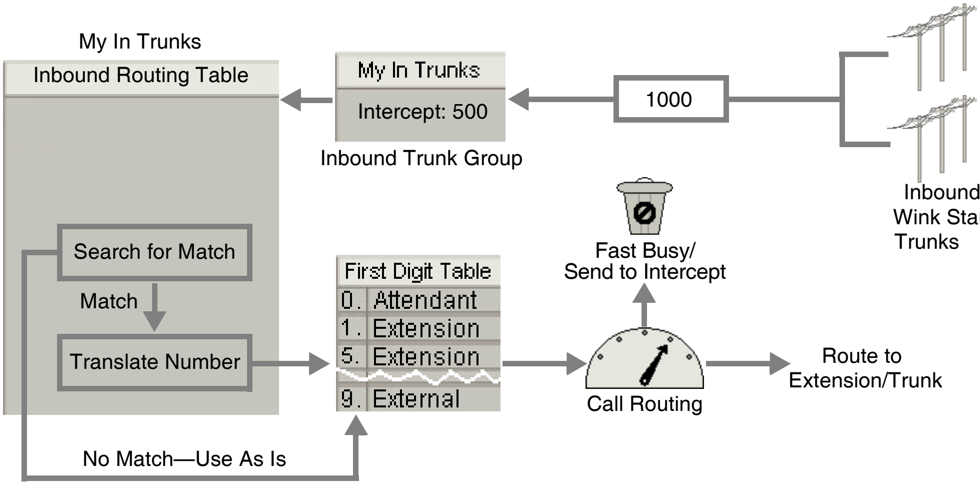
If there is no match between the number received and the steps in the table, the number is sent, as is, to the First Digit Table for further interpretation and routing. If the call cannot be routed, it will be sent to the intercept destination configured in the inbound trunk group.

Intercept destination

The intercept destination is used to intercept calls that cannot be routed. For example, if you have a block of DID numbers, 1000-1999, but you are only using 1001-1075, any call to numbers 1076-1099 will be sent to the intercept destination, if you specify one (commonly the AutoAttendant (550), or Attendant hunt group (0)). If you do not specify an intercept, the caller will hear a fast busy tone.

ISDN trunks

ISDN sends all the digits in the dialed number at once in the setup message; however, the length of digits received may vary. The following diagram illustrates ISDN inbound call routing details:



In this case it is best to enter *Default* for the Dialed Number and *2xxx* for the Destination, as shown in . This tells the PBX to keep the last three digits and prepend a 2, regardless of how many digits are received.

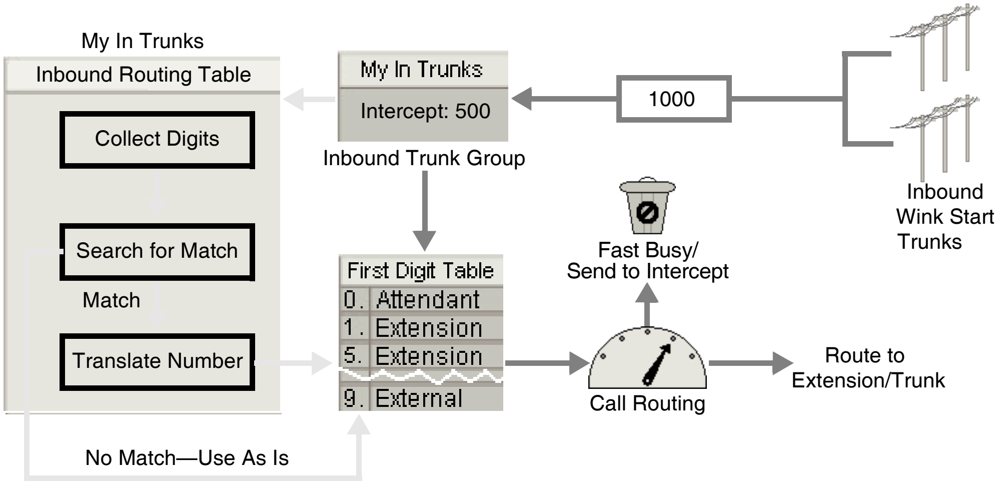
The following table illustrates a sample inbound routing table:

Step	Dialed Number	Destination	Description
1	Default	2xxx	AutoAttendant

Trunks receive digits from another PBX

When the inbound trunks receive digits from another PBX, digit translation should be handled by the PBX sending the digits, therefore no translation is necessary. In this case you should send the digits straight to the First Digit Table for digit collection and interpretation.

The following diagram illustrates Receive digits from another PBX inbound call routing details:



Tandem call routing

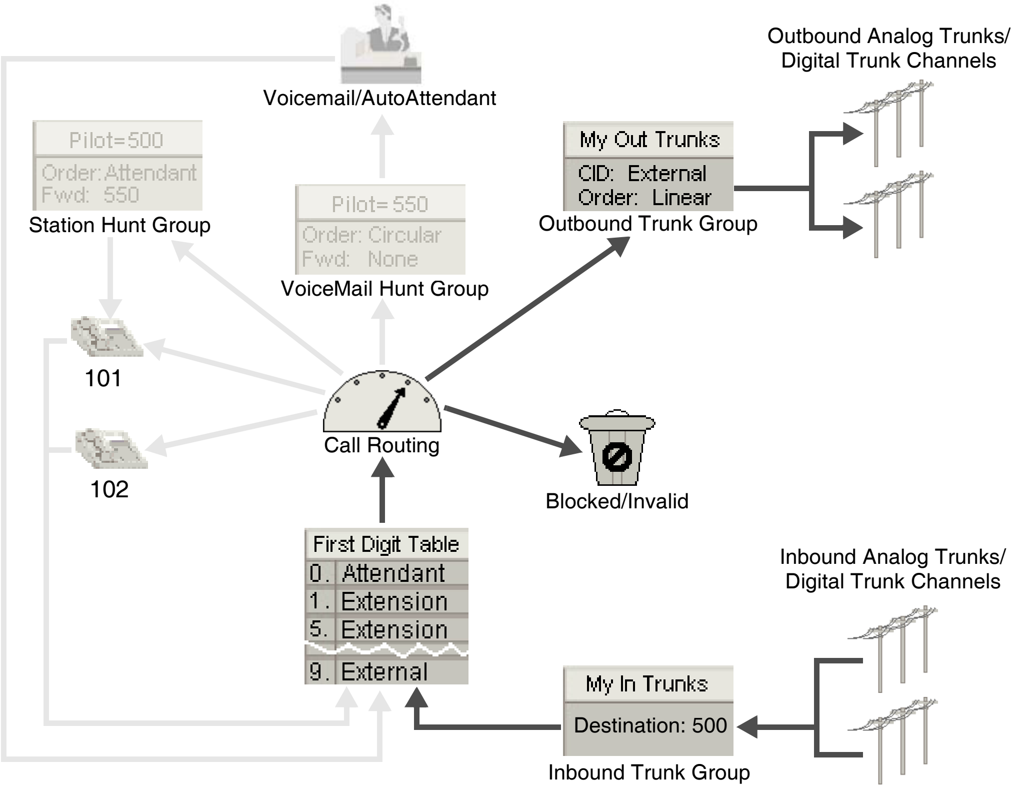
A special flavor of inbound call routing is tandem call routing. Tandem calls are inbound calls to Wave that are routed to external phone numbers. The figure below illustrates the tandem call route.

Tandem call routing scenarios include tie-line external calls (where another PBX is sending the digits for an external call), off-site call forwarding, off-site transferring, and conferencing where two or more parties are external.

This section only discusses the configuration for a tie-line external call. The tie-line external call variety of a tandem call is accomplished by relying on the calling PBX to send all the digits necessary to route the call, including the external access code (default 9), and then using the local Wave outbound call routing configuration to route the call back out on an outbound trunk group. You must configure the inbound trunk group to use the First Digit Table for digit interpretation, and specify an access profile for tandem calls. When the digits are passed to the First Digit Table, Wave picks up the associated access profile and attempts to route the call according to the call routing configuration associated with the first digit in the received number.

Other critical gateways are to enable the trunk-to-trunk connection and set the trunk-to-trunk connection time-out in the General Settings applet. See “Configuring external call routing restrictions” on page 16-14 for more information about these settings.

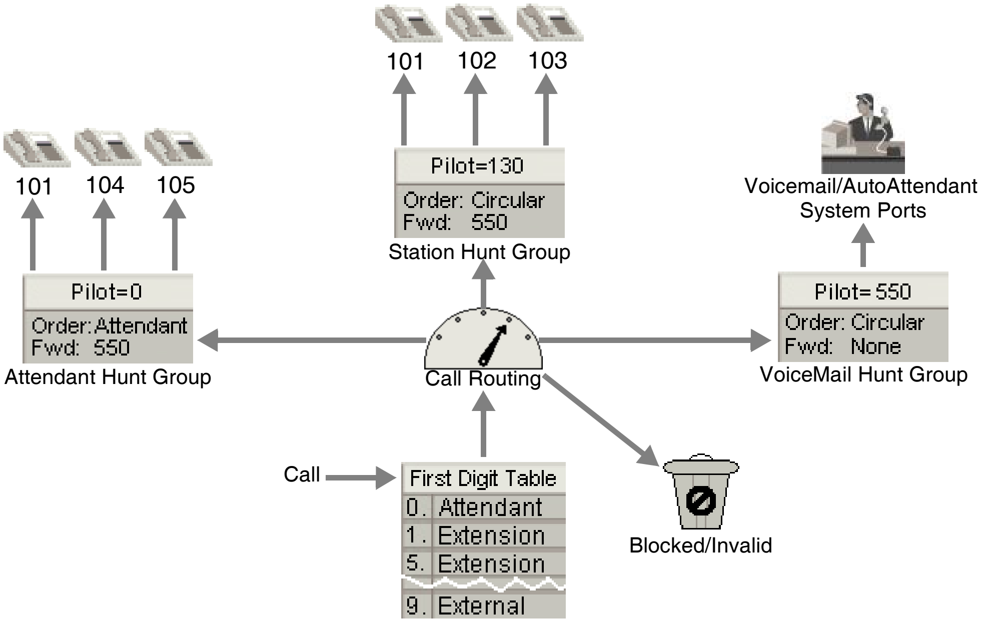
The following diagram illustrates a simplified tandem call routing scenario:



Hunt groups

A hunt group is a container extension (pilot number) that allows you to associate many user extensions or system ports to a single number that can be dialed or to which calls can be routed. When the hunt group pilot number is dialed, the hunt group configuration determines the order in which the member extensions or ports are dialed. For example, the Attendant hunt group has pilot number zero by default. If you dial zero, the member extensions of the Attendant hunt group phones will ring in the defined order.

The following diagram shows call routing via a hunt group:



There are two types of hunt groups:

- **Station**. A collection of user extension numbers. You will typically use this hunt group type for all of the hunt groups in your office, such as a group of administrative assistants or a sales group (see Pilot=0 and Pilot=130 in the figure above).

  You can include a member in more than one station hunt group. See extension 101 in the attendant and station hunt groups (pilot=0 and pilot=130) in the figure above.

- **Application**. A collection of system ports for voicemail, or other Vertical Communications applications, such as Call Navigator (see Pilot=550 in the figure above).

Hunt group hunt orders

The hunt order of a hunt group describes the order in which the member extensions ring. You can set linear, circular, ring, and attendant hunt orders.

- **Linear**. Rings the first available extension in the hunt group, always starting from the top of the hunt group list. If the first extension does not answer, the PBX rings the next available extension in the hunt group. If the second extension does not answer, the PBX rings the first extension again. If no one answers the call the caller is transferred to the hunt group’s no answer forward destination. If all member extensions are unavailable the call is transferred to the busy forward destination.

- **Circular**. Rings the member extensions of the hunt group in order until the call is answered, or all available extensions are rung (see Pilot=130 in the previous diagram). The next call to the hunt group call rings the extension following the last extension that answered a call (or the last extension before the call was transferred to the forward destination).

  For example, the station hunt group pilot number 130 in the previous diagram has three members: extensions 101, 102, and 103. When a call goes to hunt group 130, the PBX dials extension 101. If it is available, it will ring. If extension 101 answers the first call, the next time a call goes to hunt group 130, the PBX attempts to ring extension 102 first, then extension 103, and then extension 101 again. After each available extension is rung once, and no one answers the call, the call is forwarded to the no answer forward destination.

- **Ring All**. Rings all member extensions at the same time and connects the call to the first extension that answers.

  This hunt order is valid for station hunt groups only.

- **Attendant**. Hunt group members with the Attendant hunt order (see Pilot=0 in the previous diagram) are typically stations that can handle multiple calls simultaneously. If all members of a group have at least one call, the call is assigned to the first member found with the greatest number of available lines. In the case of a tie, the hunt group assigns the calls in a fashion similar to a hunt group with a Circular hunt order.

  If a member using a standard phone is in an Attendant hunt group and currently on a call, the member will hear a call waiting tone and the call will be queued to that extension.

  This hunt order is valid for station hunt groups only.

Default hunt groups

The default hunt groups are preconfigured. These hunt groups use the default system and user extensions as their members. There are three default hunt groups:

- **Attendant (station)**. The Attendant hunt group uses the pilot number zero (0). The purpose of the Attendant hunt group is to direct calls to one or more extensions that serve as the receptionists in your organization.

  By default, the Attendant hunt group has no members. By adding the member extensions you want to serve as the receptionist(s) at your site, you can connect incoming trunks to the Attendant hunt group.

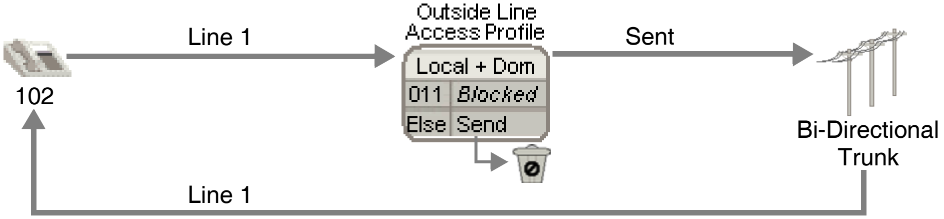
Caution! *It is not recommended that you route inbound calls to zero because there can be no voice mailbox associated with this destination.*

- **Modem Hunt Group (station)**. This hunt group (pilot 570) is used to connect incoming trunks to the modem(s) on the Integrated Services Card by setting the 570 pilot number as the default destination for the Modem trunk group. This trunk group ensures that any trunk group using 570 as the default destination will ring the first available modem.
- **Voicemail (application)**. The VoiceMail hunt group (pilot 550) is a collection of system ports. Each member of the VoiceMail hunt group is a single voicemail port that is used to play voicemail menu prompts and messages. When anyone dials the VoiceMail hunt group pilot number, they are connected to a voicemail port. The VoiceMail hunt group hunts for system ports in a circular fashion.

Outside lines

Outside lines are used to make outbound and receive inbound calls. Outside lines are ideal for users who are already familiar with a key system environment, or users who want to see the status of trunks on their digital phones. Outside lines connect a digital phone directly to a trunk using an Outside Line feature button. The routes created between the Outside Line buttons on each digital phone and trunks simulate a key system.

The following diagram illustrates an outside line:

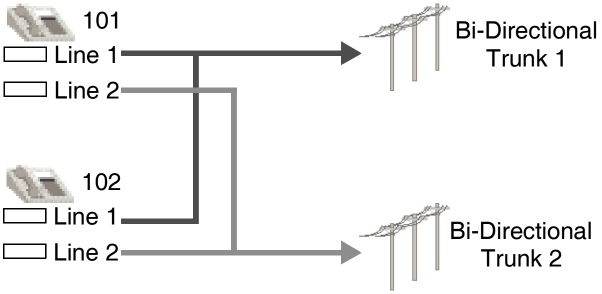


As shown in this diagram (and in the diagrams illustrating single call and multiple call variants below), the outside line buttons from each phone are linked to one or more trunks.

Outside lines can be associated with one or more trunk lines. The single call variant of an outside line requires one Outside Line feature button on a digital phone to be associated with one trunk. In the multiple call variant of an outside line, an Outside Line feature button is associated with more than one trunk. There is a significant difference in the user experience between the single and multiple call outside line variants.

Single call variant

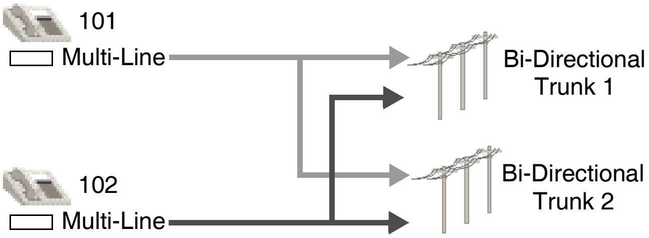
The following diagram illustrates a single call outside line variant:



In the single call outside line variant a single trunk is associated with an Outside Line feature button on a digital phone. The LED next to the Outside Line button indicates when the trunk is in use by any phone. For outbound calls, when a user presses the Outside Line button, the LED is lit red where it appears on other phones, and cannot be used on any other phone. Once the call is connected the LED indicates whether break-in is allowed. For inbound calls, the Outside Line button LED flashes yellow, and the phone can be configured to ring. Once the call is answered the LED indicates whether break-in is allowed.

Multiple call variant

The following diagram illustrates a multiple call outside line variant:



In the multiple call outside line variant an Outside Line feature button on a digital phone is associated with more than one trunk line. If any trunk line is available for outbound calls, the Outside Line button LED will not be lit on any phones with the button. The LED next to the Outside Line button is red when all of the associated trunk lines are in use. For inbound calls, the Outside Line button LED flashes yellow, and the phone can be configured to ring. When the call is connected, if there are any available trunk lines the Outside Line button LED will not be lit. If no trunks are available the LED is red. Break-in is not supported in the multiple call variant.

Automatic Line Selection

Automatic Line Selection changes the behavior of your digital phone lines (primary line, secondary line appearances, and outside lines) by allowing you to automatically answer a call that is ringing on one of those lines, or providing dial tone on the first available line, without pressing the line feature buttons.

The following rules apply to Automatic Line Selection:

- Your primary line is always subject to Automatic Line Selection behavior.
- Lines configured for Automatic Line Selection are selected in the order they appear on the phone. However, note that when you configure the feature buttons on a digital or SIP phone, you can specify that the primary line is always selected first when a user answers a ringing line or goes off-hook, regardless of where the Primary button appears on the phone. See “Primary feature” on page 10-27.
- When one or more lines are ringing, and you lift the handset or press Speaker/Mute, the first ringing line configured for Automatic Line Selection is answered.
- When no lines configured for Automatic Line Selection are ringing, and you lift the handset, press a digit, or press a feature button (Speaker/Mute, Auto Dial, System Speed Dial, Redial, Message Waiting, or Flash) you receive dial tone on the first idle line configured for Automatic Line Selection.

If you have outside lines configured with Automatic Line Selection:

- Pressing an external access code (or using an Auto Dial feature button or System Speed Dial number including an external access code) provides dial tone on the first idle outside line configured for Automatic Line Selection.

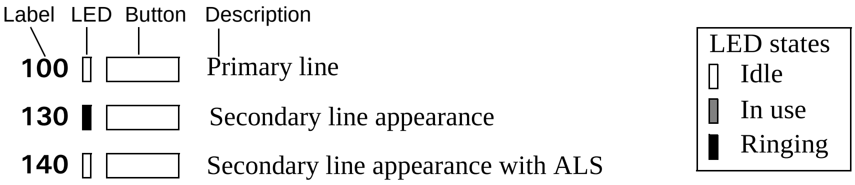
Automatic Line Selection on line appearance feature buttons

The examples that follow all use the same digital phone line feature button configuration shown in the diagram in Example 1, below.

- The first button is the primary line button configured for extension number 100.
- The second button, 130, is a secondary line appearance that is not configured for Automatic Line Selection.
- The third button, 140, is a secondary line appearance that is configured for Automatic Line Selection (ALS).

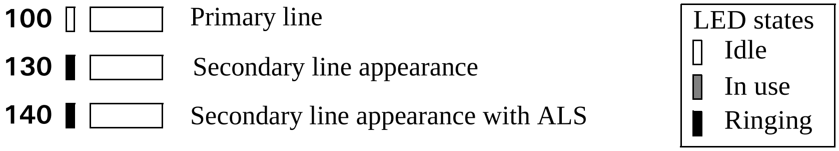
Example 1: Secondary line without ALS ringing

In the following diagram, line 130 is ringing, and is not configured for Automatic Line Selection (ALS). Lifting the handset, or pressing Speaker/Mute, pressing Auto Dial, Redial, or Flash selects the primary line.



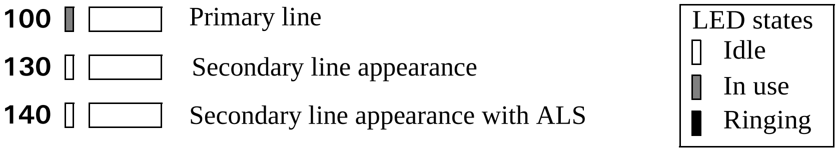
Example 2: Secondary line with ALS ringing

In the following diagram, both lines 130 and 140 are ringing. Lifting the handset, or pressing Speaker/Mute, answers the call on 140. Pressing Auto Dial, Redial, or Flash selects the primary line.



Example 3: Primary line in use

In the following diagram, the primary line is in use by another phone. Lifting the handset, or pressing Speaker/Mute, selects line 140. Pressing Auto Dial, Redial, or Flash also selects line 140. To select line 130, you must press 130.



Automatic Line Selection on Outside Line feature buttons

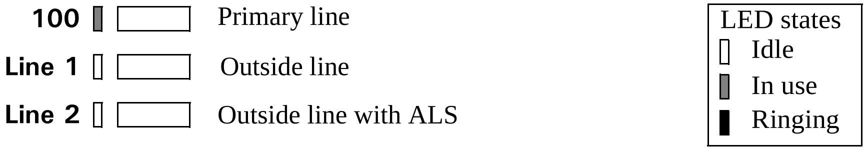
The examples that follow all use the same digital phone line feature button configuration shown in Example 1, below.

- The first button is the primary line button configured for extension number 100.
- The second button, Line 1, is an outside line that is not configured for Automatic Line Selection.
- The third button, Line 2, is an outside line that is configured for Automatic Line Selection (ALS).

Example 1: Primary line in use

In the following diagram, In the following diagram, the primary line is in use.

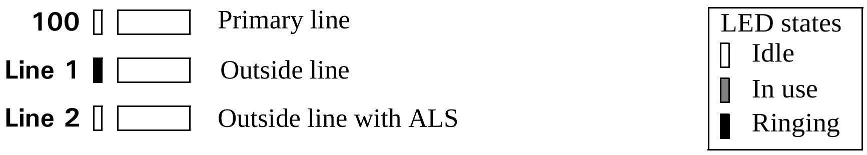
Lifting the handset, pressing Speaker/Mute, or dialing the external access digit selects Line 2. Pressing Auto Dial, Redial, or Flash produces no result. To select Line 1, press Line 1.



Example 2: Outside line without ALS ringing

In the following diagram, Line 1 is ringing.

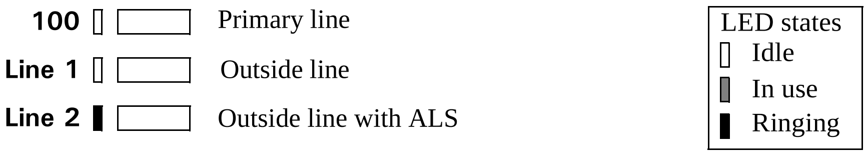
Lifting the handset, or pressing Speaker/Mute gives you dial tone on extension 100. Pressing Auto Dial, Redial, or Flash also selects extension 100. Dialing the external access digit selects Line 2. To answer the call on Line 1, you must press Line 1.



Example 3: Outside line with ALS ringing

In the following diagram, Line 2 is ringing.

Lifting the handset, or pressing Speaker/Mute answers the call on Line 2. Pressing Auto Dial, Redial, Flash, or dialing the external access digit selects extension 100. To select Line 1, you must press Line 1.



Chapter 30

Understanding Wave Data Networking

CHAPTER CONTENTS

Wave provides full routing support. The network data subsystem interfaces with network-based applications, such as Web and email servers, and communicates with the Ethernet drivers. The Microsoft Windows server/operating system embedded in Wave integrates fully with core applications, processes, and hardware.

WAN technology

Using a single WAN trunk for voice, the Wave Server provides multiple WAN services, including access through T-1 digital, ISDN PRI, and analog connections.

Network services

Wave uses the following Microsoft Windows services for communications routing:

- Routing and Remote Access Service (RRAS)
- Dynamic Host Configuration Protocol (DHCP)
- Windows Internet Name Service (WINS)
- Domain Name Service (DNS)

Microsoft's Routing and Remote Access Service (RRAS)

RRAS is Microsoft's open, extensible platform for routing and internetworking, offering LAN-to-LAN networking and remote office connectivity over private wide-area networks (WANs) or via the Internet using secure, virtual private networks (VPN).

You will configure much of Wave's data configuration via RRAS, including configuring RRAS *interfaces* (representations of connections over a network adaptor) and *adaptors* (representations of the physical point of attachment to a network segment).

Note: For detailed information about RRAS, see the Microsoft Windows NT *Routing and Remote Access Service Administrator's Guide*.

The Wave LAN, segments, and subnets

When a network is composed of hubs and routers, segments and subnets are essentially the same. When designing your network, follow these rules:

- Each port on a router has to be on the same subnet as all machines to which it is connected.
- A machine's subnet has to match that of the router closest to it.
- Only routed packets are propagated from one hub to another.

Note: A single switched Ethernet domain is faster and requires less system resources then routing between segments.

Note: It is acceptable to configure an Integrated Services Card (ISC1) or VAM with multiple IP addresses, and for the card to have multiple subnets. While it is sometimes useful to preserve a pre-Wave configuration, we recommend that you do not do this normally, as it can be confusing to administer.

Dial-up and persistent connections

The Wave Server supports various kinds of dial-up and persistent connections.

Dial-up connections

A *dial-up connection* is created and ended on an as-needed basis. A dial-up connection typically has a phone number associated with it. The connection is made only when a phone call connects the Wave Server with an ISP or with a corporate headquarters over a WAN. A dial-up connection (also known as a switched connection) is the RRAS default.

Using ISDN or the modem port(s) on the Integrated Services Card, you can configure the Wave Server for dial-up connections, routing data using Microsoft RRAS. Both Wave modems and ISDN serve as system resources for dial-in and dial-out calls.

Dial-in calls come from a remote office over a digital or analog trunk *to* Wave. Modems and ISDN are configured so that remote dial-in calls will automatically connect through the Wave Server.

Dial-out calls are made *from* Wave over a digital or analog trunk to an Internet Service Provider or to another site. The type of dial-out calls made when a user requests an Internet connection, known as dial-on-demand or *demand-dial calls*, depends on trunk type and protocols in use, as well as modems, and can be set up through the RRAS administrator application.

Caution! *Do not set an interface for dial-on-demand if you intend to use it for continuous monitoring of the Wave Server. If the monitoring traffic is high, the connection will never be disconnected. In addition, if you are monitoring the Wave Server using SNMP over the dial-on-demand connection when the connection is disconnected, this will generate an SNMP trap causing the connection to be reconnected. The end result is that the connection will continually be going up and down.*

Note: The Wave Server supports *dial-on-demand*, also called dial backup, over analog phone lines. If a digital line fails, a dedicated 2400-baud modem automatically dials a pager over analog lines on system failure.

Wave dial-in connection default settings

The modem on the Wave Server are set up for configurable dial-out functionality and to automatically answer incoming calls to the default Modems hunt group (extension 570). When a client machine dials in, the default Modem trunk group rings the default Modems hunt group. The Modems hunt group rings the modems in a circular fashion until it finds a free modem extension to answer the dial-in call.

Note: For calls from outside Wave to connect, the Modems hunt group extension must be bound to a phone number that can be reached from outside Wave.

Persistent connection

A *persistent connection* is always logically and physically active. It may also be referred to as a dedicated account. While the connection is intended to be constantly active, the physical connection may be disconnected if the Wave Server is restarted.

The Wave Server also supports a persistent ISDN connection.

A persistent connection may be a *permanent connection*—both physically and logically active—such as a digital line that goes to your ISP. All permanent connections are persistent.

Wave data routing

A *router* is a device that moves data packets between networks. A router can be used to link LANs together, locally or remotely, as part of a WAN. *Routing* is the process of delivering messages from the sender to the receiver using the most appropriate path through one or more networks.

The Wave Server uses RRAS, a software router, as a LAN-to-LAN, LAN-to-WAN, and WAN-to-WAN router for IP traffic. RRAS IP routing is installed and enabled by default, so LAN routing configuration is, for the most part, automatic. Depending on your particular Wave configuration, you may need to configure routing protocols and/or LAN-to-WAN interfaces.

You can configure routing protocols, including the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), as well as default and static routes, on Wave when multiple routers are connected to your network. You can also configure Internet Packet Exchange (IPX), which uses the routing protocols RIP and SAP, as an alternative to IP.

Note: By default, these routing protocols are installed but not configured, as they are not required for typical configurations. If you need to configure these, see “Configuring network routing protocols” on page 21-3.

IP addressing

All network interfaces on Wave must have valid *static* IP addresses assigned, even if Wave is connected to a network server. In determining IP addresses, follow these guidelines:

- For your network interfaces, use the standardized, unregistered, non-connecting IP addresses set aside in RFC 1918, “Address Allocation for Private Internets.” RFC 1918 is published by the Internet Engineering Task Force (IETF); the IETF web address is http://www.ietf.org.

  RFC 1918 includes the following addresses:

  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255
- Do not assign IP addresses ending in .0 or .255 to individual machines, as these are the network and broadcast addresses for Class C addresses.

Each Wave Server needs a minimum of 2 static IP addresses—one for the Integrated Services Card (ISC) and one for the VAM. In addition, if an MRM is installed in the Wave Server, additional IP addresses will be needed (up to 3 depending on the MRM model) . For details, see “Configuring the administrator PC” in Chapter 5 in the *Wave Server Installation Guide*.

- The default IP address for the VAM is 192.168.205.1 and the default Subnet Mask is 255.255.255.0.

- The default IP address of the ISC is 192.168.205.10 and default Subnet Mask is 255.255.255.0.

The following are additional guidelines for working with IP addresses and subnet masks:

- Router interface IP addresses typically end in .1. For example, if subnet 1 is 192.168.3.*, its network interface IP address would be 192.168.3.1; if subnet 2 is 192.168.4.*, its network interface IP address would be 192.168.4.1, and so on.
- Use the next logical number that is not currently assigned to assign new IP addresses.
- If your Wave Server is connected to an external DHCP server, modify the Wave default IP addresses to use an IP address within the server’s subnet range. For example, if the DHCP server address is 204.1.1.1, you might change the Integrated Services Card address from 192.168.1.245 to 204.1.1.245, and set the Wave IP address range from 204.1.1.2 to 204.1.1.244. You must set this address, because the Wave Server cannot be a DHCP client.

- You can assign multiple IP addresses to any router port/network interface, as long as there are not two machines with the same address on the same network.
- In general, a host route subnet mask is 255.255.255.255 and is used for referring to a single machine; a default static route subnet mask is 0.0.0.0; and a subnet mask is in between the host and the default, typically with an address of 255.255.255.0.
- The default gateway address, which answers the question “Who do I contact when a machine is not on my subnet?,” is that of the closest router on the subnet. If the network interface address is x.x.3.1, the default gateway address is x.x.3.1. Ask your network administrator for the appropriate address.

Using a proxy server with Wave

Proxy servers convert private IP addresses to public IP addresses for sending packets over the Internet. If your network uses private IP addresses (such as the default Wave IP addresses), you can use a proxy server or a network address translator (NAT) to perform IP address translation.

- If your network has an existing proxy server, connect one network interface of the Wave Server into the subnet containing the proxy.
- If you have no existing proxy server, create a subnet on which you put all your internet services—such as proxy server, mail server, and Web server—with official IP addresses. Set up a separate subnet for all machines using unofficial IP addresses as proxy clients.

Routing protocols

Routing protocols implement dynamic routing, modifying paths as needed, taking advantage of more efficient routes, and avoiding broken networks. Routing protocols are used by routers to communicate current routing information to other routers and to workstations using these routers. They allow an end-to-end path for packets to be chosen, while only requiring each router to know the path to the next router. The routing cost of a path is measured by a metric, and the least expensive path is always chosen.

Routing Information Protocol (RIP)

Routing Information Protocol, or RIP, is used to discover all the subnets on a network dynamically, communicate when a subnet goes down, and rediscover the subnet when it comes back up. Routers configured for RIP send announcements frequently to update routing tables. The RIP protocol can run on top of either IP or IPX. If you configure IPX, RIP is automatically configured for you.

Note: RIP version 1 is not aware of network masks (subnets), and instead uses class A, B, and C addresses to determine routing. If you are using RIP version 1, be sure to make all IP addresses parallel in size.

RIP uses the shortest number of hops to send a packet from point A to B, but does not take the speed of connection lines—digital versus modem versus ISDN, for example—into account when it is routing.

Open Shortest Path First (OSPF) routing protocol

The Open Shortest Path First (OSPF) dynamic routing protocol takes bandwidth into account when forwarding packets. OSPF will automatically choose a digital line over an ISDN line, for example. OSPF will route overloaded packets on the shortest path, and will use a second digital line when one is available, although you still have to calculate the metrics OSPF should use.

Use OSPF if the Wave Server is part of a large, hierarchical network with redundant paths or backbone routers.

Internet Packet Exchange (IPX)

When you are running Novell NetWare services on your Wave network, you will need to configure Internet Packet Exchange (IPX) on Wave. IPX is Novell NetWare’s native LAN communication protocol. All Microsoft Windows and NetWare interoperability services rely on IPX to communicate with NetWare servers.

IPX supports a simple address scheme that allows clients to communicate with servers residing in other logical networks, and lets routers determine what traffic needs to flow between different links. IPX does not dictate that each client and server have assigned addresses, other than the physical network adapter address. (In contrast, TCP/IP requires every client and network to have a unique assigned address, with both a network component and a system address.)

Microsoft Windows Server 2003 accommodates TCP/IP and IPX, individually or concurrently. What you configure depends on your particular network configuration.

Routing protocol metrics

All IP addresses, subnet masks, and metrics are stored in a routing table so that packets of information can be directed quickly to their destinations. If a client on a subnet sends a packet to another on the same subnet—x.x.3.3 to x.x.3.8, for example—the packet goes directly to its recipient. If a client on one subnet sends a packet to a client on a different subnet—x.x.3.3 to x.x.4.9, for example—the packet is sent through a router, and is routed along the shortest path from one point to another, based on routing protocol metrics.

Routing protocol metrics measure the cost of sending a packet between a source and a destination. By setting routing protocol metrics, you can define pathways and alternate pathways for routing packets.

Hint: The IP Routing Table in the RRAS administrator reports non-local metrics as one greater than they really are.

The RIP metric, for example, is measured in hop counts (the number of nodes, composed of routers and other devices).

The OSPF metrics take bandwidth and load sharing (distributing bandwidth across equal paths) into account, making them both more advanced and more complex to configure than RIP metrics.

Note: Backup routing requires special configuration, since RRAS cannot detect link failures. The digital link must have RIP or OSPF configured, and the modem link must have a default or static route configured.

Static routes

In a small (single subnet) network environment, particularly with only one point of entry to the Internet, you can use static routing instead of configuring RIP or OSPF. In static routing, the routes do not change once you set them. However, this also means that if any network failures occur, there are no other paths available in the network to route around the failure.

The Wave Server uses RRAS, a software router, as a LAN-to-LAN, LAN-to-WAN, and WAN-to-WAN router for IP traffic. RRAS IP routing is installed and enabled by default, so LAN routing configuration is, for the most part, automatic. Depending on your particular Wave configuration, you may need to configure routing protocols and/or LAN-to-WAN interfaces.

Routing protocols for static routes

The Wave Server supports two protocols for dynamic routing: RIP and OSPF. Without RIP or OSPF enabled, IP only forwards packets between static routes on subnets. In addition, the Wave Server supports IPX for routing between Novell NetWare servers.

For information about configuring RIP, see “Configuring routing information protocol (RIP)” on page 21-3.

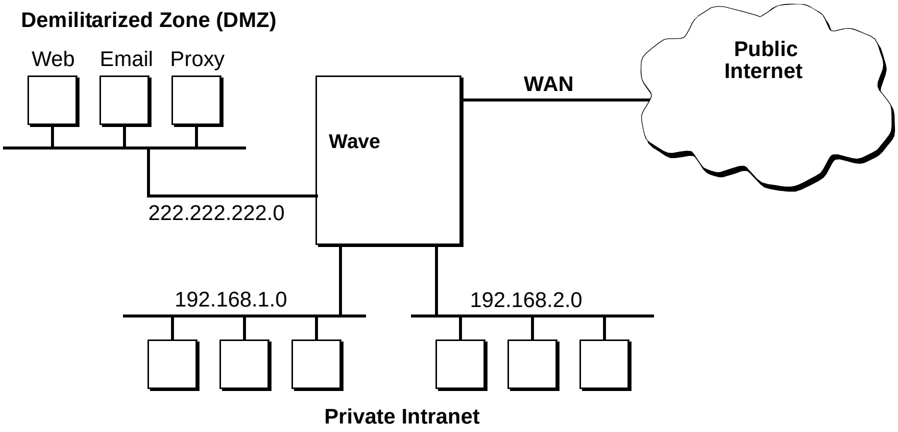
Packet filtering

Packet filtering is a way of restricting network traffic on an interface to just those packets that match a given pattern. This is typically done to provide a level of security against untrusted networks (such as the Internet) or to conserve bandwidth on WAN interfaces.

Since the patterns are fairly simple, packet filtering does not afford the same level of security or configuration as a network firewall or proxy. However, it is sufficient for many environments, and can also be used in addition to more sophisticated methods. Packet filters in Wave only support the Internet Protocol (IP) and those that utilize IP, such as TCP, UDP, and ICMP.

The following sections describe packet filters and how to use them in different environments. In many cases, multiple environments might apply. For example, Wave can support one or more interfaces with filters for a private network, a DMZ network, the Internet, and port filters.

The following illustration shows a sample network with public, private, and DMZ areas, where Wave is connected to the Internet over a WAN, the private network consists of 192.168.1.0 and 192.168.2.0, and the DMZ is 222.222.222.0.



DMZ networks

A DMZ (De-Militarized Zone) network is where publicly-accessible servers are typically located, such as Web servers and email servers. More importantly, in an environment with a private network (see “Private networks”), only machines in the DMZ communicate directly with the Internet.

To enforce this security, properly constructed packet filters will:

- Allow the DMZ to communicate with the Internet
- Reject any direct communication between the private network and the Internet
- Optionally restrict communication between the DMZ and the Internet to particular services
- Optionally restrict communication between the DMZ and the private network to particular services

This section discusses the first two goals, which are enough for most environments. The latter two goals are covered in “Protocol and port filtering of common services” on page 30-14, and should be used in environments where security is an important issue.

To allow communication between the DMZ and the Internet, only two cases should be allowed:

- Packets sent by a DMZ address going out to the public Internet
- Packets sent to a DMZ address coming in from the public Internet

The following filters can be put into place on the WAN connection(s) with the filters set to "drop all except listed below." The IP addresses in the following table are those for the sample network illustrated in the diagram in "Packet filtering" on page 30-10; substitute the addresses for your own DMZ as appropriate.

DMZ network filters (drop all except those listed below)

Direction	Filter Type	IP network address	Subnet mask
Input	Destination network	222.222.222.0	255.255.255.0
Output	Source network	222.222.222.0	255.255.255.0

Private networks

A private network (often referred to as an intranet) often uses RFC 1918-allocated, unregistered IP addresses—sometimes known as private networks—which are used by a large number of networks worldwide, with the understanding that they will never transmit those addresses on any public network. If a company wishes to then connect to the public Internet, a network proxy or Network Address Translator (NAT) is used to convert between the two sets of IP addresses. This is done both for security and to avoid obtaining public, registered IP addresses to simplify administration of the company's network. In an environment such as this, care should be taken to avoid communication between the two networks.

In a simple environment, routing information is not passed between the ISP and the private network. Therefore, the private network must have a default route (0.0.0.0 / 0.0.0.0) directed at the ISP. A side effect is that any traffic that is not terminated internally (such as traffic destined for a subnet that had just gone down) would be routed to the ISP.

Generally, the public Internet will not be able to handle the private IP addresses, and they will eventually be discarded by one of the ISP's routers. This alone ensures that there is no normal communication between the two networks.

However, there are a few reasons to place a firewall between the two networks:

- Increased security; while it is an extreme case, a hacker who has direct access to your ISP could get around the discarding of your private addresses
- Lessen the traffic across the WAN connection to the ISP
- Consideration to your ISP by not giving them additional unnecessary traffic

Normally, however, the private intranet will use the services of a network proxy or NAT which is located in the DMZ network, and will never communicate with the untrusted Internet directly. Therefore, the DMZ packet filters will accommodate all of the above goals, and only those filters are needed.

To create a firewall between the public and private networks, four cases must be prevented from passing across the WAN. The latter two cases may seem redundant, but should be put in place to provide maximum security.

- Packets sent by a private network address going out to the public Internet
- Packets sent to a private network address going out to the public Internet
- Packets sent by a private network address coming in from the public Internet
- Packets sent to a private network address coming in from the public Internet

These filters can be put in place by either Wave or the ISP. If this firewall is a serious concern for your company, then the filters should be enabled on Wave; if you wish to lessen administration, let the ISP enable the filters.

The filters listed in the following table can be put into place on the WAN connection(s), with the filters set to receive/transmit all except listed below. Each of these filters should be added as both input and output filters, thereby creating a total of 12 filters. You can use all of them, or just the subset matching your private addresses. These filters are listed with the IP network address and then the subnet mask.

Outbound and inbound filters

Direction	Filter Type	IP Network Address	Subnet Mask
Input/Output	Source	10.0.0.0	255.0.0.0
Input/Output	Source	172.16.0.0	255.240.0.0
Input/Output	Source	192.168.0.0	255.255.0.0

Outbound and inbound filters

Direction	Filter Type	IP Network Address	Subnet Mask
Input/Output	Destination	10.0.0.0	255.0.0.0
Input/Output	Destination	172.16.0.0	255.240.0.0
Input/Output	Destination	192.168.0.0	255.255.0.0

Protocol and port filtering of common services

The most specific type of filtering is known as protocol filtering or port filtering. This allows only specific protocols on an interface. For example, you may wish to disallow FTP over your connection to the Internet. These types of filters can be complex to set up and maintain.

Wave packet filters can only perform simple filters on the protocols, since they are not dynamic nor do they track the state of the connection. A more sophisticated firewall or network proxy is needed for complex environments and protocols.

A common practice is to limit access to the Internet to only a few different services and ports. This is fairly straightforward if there are no Internet servers (such as web or email) located on-site. To do this, you would set up a “dump all except listed below” filter which allows only specific protocols and ports.

Typically, this list includes the TCP and UDP services listed in the following table. This is a subset of what is referred to as **well-known port numbers**, which is documented in various places, such as STD 0002 (also known as RFC 1700). While most services’ ports are valid for both TCP and UDP, in practice you will probably only see one or the other.

Common ports for TCP and UDP

Service	Port	Full Name
DNS	53	Domain Name Services
FTP	20, 21	File Transfer Protocol
Gopher	70	Gopher
HTTP	80	World Wide Web HyperText Transfer Protocol
IMAP4	143	Interim Mail Access Protocol, Version 4

Common ports for TCP and UDP

Service	Port	Full Name
NNTP	119	Network News Transfer Protocol
POP3	110	Post Office Protocol, Version 3
PPTP	1723	Point-to-Point Tunneling Protocol (See “PPTP filtering” on page 30-16 for additional information)
Remote Desktop	3389	Remote Desktop
SMTP	25	Simple Mail Transfer Protocol
Telnet	23	Telnet

The list of desired services could also include the ICMP protocol, which allows ping and TRACERT to work. For simplicity, you can specify just the ICMP protocol and leave the type and code fields blank, which will allow all ICMP through. However, you could only allow ICMP type 8 (echo request) to be output and both ICMP type 0 (echo reply) and type 11 (time exceeded) to be input; this would allow you to ping the Internet, but no one on the Internet could ping you. A list of ICMP message types is supplied in the following table.

ICMP message types

Type	Description
0	Echo reply
3	Destination unavailable
4	Source quench
5	Redirect
8	Echo request
9	Router advertisement
10	Router solicitation
11	Time exceeded
12	Parameter problem

ICMP message types

Type	Description
13	Time stamp request
14	Time stamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

As an example, you could create an environment where only web browsing was permitted, by filtering out all protocols except for DNS and HTTP. To do this, the following filters can be put into place on the WAN connection to the Internet, with the filters set to drop all except those listed below.

Protocol filters for Web browsing (drop all except those listed below)

Direction	Filter Type	Protocol	Direction	Port
Input	Protocol	UDP	Source port	53
Input	Protocol	TCP	Source port	80
Output	Protocol	UDP	Destination port	53
Output	Protocol	TCP	Destination port	80

PPTP filtering

In some environments, a network may only be used for tunneling, but not for actual traffic. For example, a branch office may use PPTP to tunnel through the Internet to headquarters, but may not use it for anything else. More commonly, the interface has protocol filters in place, and you can allow PPTP traffic, allowing home users to tunnel into the company’s network.

Caution! *On the Advanced TCP/IP Protocol properties windows of the Microsoft Windows Network control applet, there is an Enable PPTP Filtering option. Do not select this option.*

There are three cases in which Wave allows for PPTP:

- Packets with TCP source port 1723
- Packets with TCP destination port 1723
- Packets using IP protocol number 47, which is the Generic Routing Encapsulation (GRE) protocol

A total of six additional filters must be in place, with the filters set to drop all except those listed below.

Protocol filters for PPTP (drop all except listed below)

Direction	Filter Type	Protocol	Field	Value
Input	Protocol	TCP	Source port	1723
Input	Protocol	TCP	Destination port	1723
Input	Protocol	Other	Protocol	47
Output	Protocol	TCP	Source port	1723
Output	Protocol	TCP	Destination port	1723
Output	Protocol	Other	Protocol	47

Network services

Wave uses the following Windows services for network information services:

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name Service (DNS)
- Windows Internet Name Service (WINS)

By default, Wave does not use DHCP and can be easily configured to be a client of WINS and DNS.

Wave as DNS client

The Internet and most private networks rely on DNS to provide name resolution service to all clients and servers. Since Wave has to know how to resolve outside Internet addresses, it needs the DNS service or a proxy server. Configure Wave as a DNS client when another server in your network performs DNS services.

Wave as WINS client

Configure Wave as a WINS client when you want the WINS server to resolve client-computer requests for names mapped to IP addresses for file, print, and application traffic.

DHCP relays

If your Wave Server is connected to an external DHCP server, and you wish to use the DHCP server for the subnets connected to the Wave Server, you must configure Wave as a DHCP relay.

The DHCP relay agent is a component of RRAS. The Relay Agent allows Wave to forward requests for IP address assignment, using DHCP, from a routed subnet on one Ethernet hub card to a separate DHCP server on another subnet.

Configure DHCP relays if your clients and the DHCP server are on a different routed subnet or network.

You do not need to configure the DHCP relay agent if you have a large network with DHCP servers on each subnet. DHCP Relay will not work if DHCP Server is running on the same system.

Part 4

Reference

Chapter 31

Wave Reports

CHAPTER CONTENTS

This chapter describes how to configure, run, and interpret the following Wave system reports:

- The Call Detail Report. See page 31-2.
- The Trunk Statistics report. See page 31-14.

You can also produce a variety of useful reports via the Wave Report Generator. See “Using the Report Generator” on page 31-25 for a list of the available Report Generator reports and instructions on how to run them.

Wave ViewPoint provides an additional suite of reports on call activity and phone usage. For details, see Chapter 13 in the *Wave ViewPoint User Guide*.

The Call Detail Report

The Call Detail Report (CDR) provides a daily summary log file of all Wave incoming and outgoing calls. It can be used for validating a newly installed Wave Server and for call accounting. Used in conjunction with a front-end call accounting package or a Microsoft Excel spreadsheet designed to provide the breakdowns you need, you can sort and chart records of customer traffic by extension, duration, time of use, and so on, for departmental or customer billing.

By default, the Call Detail Report logs one day of calls in each file—approximately 650 KB, if an office makes an average of 2,000 calls per day. You set the number of files you want to save, and when Wave reaches that limit, the oldest files are deleted first. You can increase the number of files saved using the Call Detail Report applet. Use the following information to determine how many files to save:

- Each 1 MB stores approximately 2,600 call records.
- The default number of files stored is 60, or approximately 38 MB based on an average of 2,000 calls per day; the maximum number of files is 180, or approximately 114 MB, based on an average of 2,000 calls per day.

Wave supports access to CDR data through FTP. CDR data is captured and posted on the internal FTP server. Every 30 minutes the data is updated with the latest information. The frequency is set for 15 and 45 minutes after the hour every hour. Wave saves 60 days worth of files on the FTP server before replacing the oldest file with the latest file.

This section contains the following information:

- Configuring the Call Detail Report. See page 31-3.
- Call Detail Report specifications. See page 31-4. This section describes in detail the rules, formats and field descriptions for the Call Detail Report, as well as the IP telephony voice extension record.

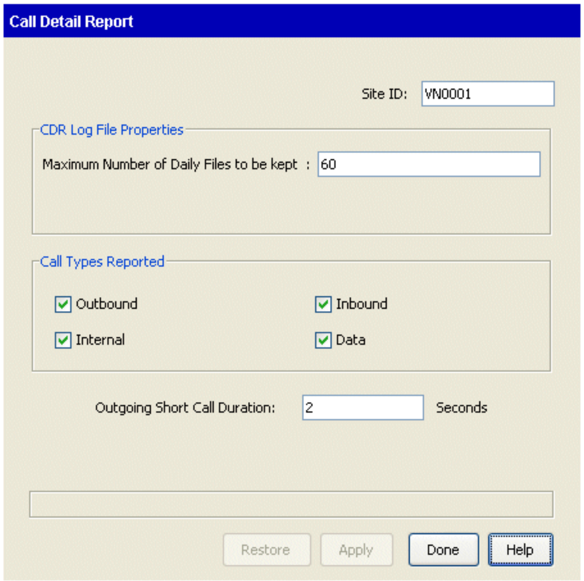
Configuring the Call Detail Report

You will typically configure the Call Detail Report once, to set the outgoing short call duration, the number of daily summary log files to save, and the type of call detail records to capture.

To configure the Call Detail Report

Click

1. If necessary, click the Administration tab of the Management Console.
2. Click the Call Detail Report icon, located in the General Administration section.
3. The Call Detail Report dialog opens.



Call Detail Report

Site ID: VN0001

CDR Log File Properties

Maximum Number of Daily Files to be kept : 60

Call Types Reported

☑ Outbound ☑ Inbound
☑ Internal ☑ Data

Outgoing Short Call Duration: 2 Seconds

4. Enter a **Site ID** if you have multiple systems and want to distinguish Call Detail Reports between systems. Up to six alphanumeric characters are allowed.
5. Type the maximum number of daily report files you want stored in the **Maximum Number of Files** field.

   The number of files is limited by the size of hard-disk storage. When limit you set is reached, the oldest files are deleted first.

Note: You might want to set the Maximum Number of Files field based on your billing cycle. For example, you are probably billed monthly, and if you take billing lag time into consideration, you might set Wave to save 60 files. You can then correlate your bill with the Call Detail Report log.

6. In the Call Types Reported section, select one or more checkboxes for the call types that you want to report on:
   - **Outbound**
   - **Inbound**
   - **Internal**
   - **Data**
7. In **Outgoing Short Call Duration**, enter the number of seconds to use to determine when to record outbound calls over trunks that do not provide answer supervision (such as analog loop start trunks). Such calls are not recorded if they are shorter than the **Outgoing Short Call Duration** that you specify.

   Setting a minimum duration distinguishes busy/ring no answer calls from completed calls in the Call Detail Report. The default is 45 seconds. The possible range is 0 to 60 seconds. If you use a lower setting, such as 30, all outbound calls (on trunks without answer supervision) that last 30 seconds or more will be recorded.
8. Click **Apply** to save your changes.
9. Click **Done** to return to the Management Console.

Note: Changes to calls types and duration settings, as well as log file property settings, are applied when you click **Apply** or **Done**; site ID is applied after you restart the Wave Server.

Call Detail Report specifications

This section describes the following:

- Call Detail record and field rules. See page 31-5.
- Call Detail record formats. See page 31-5.
- Call Detail field descriptions. See page 31-6.
- IP telephony voice extension record. See page 31-12.

Call Detail record and field rules

The Call Detail Report logs calls according to the following rules for records and fields:

- A record is logged when a call terminates.
- A single record is logged for a conference call.
- When an extension tries to make an outbound call and all trunks are busy, the call action column logs a B for all trunks busy.
- When multiple parties are involved in a call, such as a transfer, the calling party is the person initiating the call, the called party is the first person who answers the call, and the final party is the last person who answers the call. The Primary Call Record ID column provides a log of each call, tying these calls together. Call duration is the total time from the first person answering the call to the last person hanging up the call, including time spent on hold.
- In conference calls, the person who creates the conference is logged in the call ID column. One of the last two parties to leave the call is logged as the final party.
- Incoming calls begin when the attendant, voicemail, or the first extension answers a call.
- If outbound calls are shorter than the Outgoing Short Call Duration configured in the Call Detail Report applet, they are defined as unanswered, and are not recorded, unless the central office provides answer supervision. The default time is 45 seconds.

Note: Outgoing calls over analog loop start trunks do not provide answer supervision, which means that Wave cannot tell whether a call is answered when it is placed over a loop start trunk. The Outgoing Short Call Duration setting lets you establish a time after which such calls will be assumed to be connected, and will be recorded in the Call Detail Report.

Call Detail record formats

The Call Detail Report fields use the following formats:

- Records are delimited with carriage return
- Records are ASCII-based

- Fields are right-justified
- Fields are padded with blanks; the Duration and End TM fields are padded with zeros
- Fields are comma-separated

Call Detail field descriptions

Each Call Detail Report log begins with a header. Call Detail header fields are described in the following table.

Call Detail header field descriptions

Field Name (example)	Description
<HEADER>	Indicates the beginning of the log header.
FileID (Cdr)	Identifies the type of file.
Version (7.02)	Specifies the revision of the file format.
Serial Number (123456)	The Vertical Wave serial number as entered via the General Settings applet.
Hostname (nnnnn)	The name of the Wave Server.
IP Address (nnn.nnn.nnn.nnn)	The IP address of the Wave Server.
Start Date (yyyymmdd)	The date the file was created.
Start Time (hh:mm:ss)	The time the file was created.
<\HEADER>	Indicates the end of the log header.

The following table describes the Call Detail Record Log fields. Note that in a Microsoft Excel spreadsheet, columns are indicated by letters, as displayed in the **Column (Excel)** column. Also, the **Field length** column indicates the number of characters used. By default, Microsoft Excel does not display leading zeros.

Call Detail Record Log field descriptions

Column (Excel)	Field Name	Field Length	CDR Head	Description
1 (A)	**VID**		VID	Vertical ID.
2 (B)	**Call Record ID**	8	Entry	An incrementing number that uniquely identifies each Call Detail Report record, or text that identifies restart-related, non-CDR records, which are identified with an asterisk (*). Clearing a Call Detail Report log does not reset incrementing record numbers. Non-CDR records such as the Call Detail Report header and restart information (start and stop times) will have a non-numerical value in this field. Restart-related, non-CDR records include: • **Entry**. Vertical Communications header; always the first entry in the file (no asterisk). • **Cleared**. Date and time that the Call Detail Report record was cleared; always the second entry in the table. • **Stop**. Date and time Wave stopped. • Restart. Date and time Wave is able to process phone calls. • **CM Stop**. Date and time Wave stopped processing phone calls because the Connection Manager stopped.
3 (C)	**Site ID**	6	Site	System identification number, such as **VN0001**, the default. You can change the site ID; see "Configuring the Call Detail Report" on page 31-3.

Call Detail Record Log field descriptions

Column (Excel)	Field Name	Field Length	CDR Head	Description
4 (D)	**Call Duration**	8	Duration	The duration of the call in the format ddhhmmss. When multiple parties are involved, call duration is the total time from the moment the first person answers the call until the connection ends (one of the last two connected parties hangs up). Microsoft Excel strips leading zeros, so if the call was one minute, two seconds long, you would see **102**; if the call was two hours, one minute, two seconds long, you would see **20102**. Only if a call was more than 24 hours long would you see something like **1094451** (a duration of 1 day, 9 hours, 44 minutes, 51 seconds). If a call duration exceeds 100 days the field will contain **99235959**.
5 (E)	**End Date**	8	End date	The date the call ended in the format yyyymmdd, such as **20001130** for November 30, 2000. In a restart-related record, end date indicates system clear, stop, or restart date.
6 (F)	**End Time**	6	End TM	The time the call ended in the 24-hour format hhmmss, such as **140102** for 2:01:02 P.M. In a restart-related record, end time indicates system clear, stop, or restart time
7 (G)	**Call Type**	1	T	A single character that defines the type of call. Current types: • **>** = Inbound call • **I** = Internal call • **<** = Outbound call • **D** = Data call • **T** = Tandem call

Call Detail Record Log field descriptions

Column (Excel)	Field Name	Field Length	CDR Head	Description
8 (H)	**Call Action**	1	A	A single character that defines the action the call took. Actions, in highest to lowest precedence, with multiple action calls logging only the highest precedence action, include: **C** = Conference **O** = Off-site forward **F** = Forward **X** = Transfer **B** = All trunks busy **D** = Direct trunk.
9 (I)	**Access Code Dialed**	4	TACD	Reserved. Not supported in this version.
10 (J)	**Access Code Used**	4	TACU	Reserved. Not supported in this version.
11 (K)	**Call ID**	8	Call ID	The extension number defined as the owner of this call. In conference calls, the Call ID is the person who creates the conference. Having a single location for this field makes database searching easier.
12 (L)	**Calling Number**	20	Calling Party	The number of the call source, either an internal extension or an external number.
13 (M)	**1st Destination Number**	25	Called Party	The first destination of the call, either an internal extension or an external number.
14 (N)	**Final Destination Number**	25	Final Party	The final destination of the call. If the call forwards multiple times, the final destination is where the call eventually connects. In conference calls, the final destination number is one of the last two parties to leave the call.
15 (O)	**Account Code**	16	Reserved	Reserved. Not supported in this version.
16 (P)	**Authorization Code**	12	Authorize	Up to 12 digits of the user’s dialed authorization code.

Call Detail Record Log field descriptions

Column (Excel)	Field Name	Field Length	CDR Head	Description
17 (Q)	**Incoming Trunk Group Number**	8	In TKGP	The pilot number of the trunk group which received the incoming call.
18 (R)	**Incoming Circuit**	8	In TRK	The number associated with the trunk used to accept an incoming call.
19 (S)	**Outgoing Trunk Group Number**	8	Out TKGP	The pilot number of the trunk group used to place the outgoing call.
20 (T)	**Outgoing Circuit**	8	Out TRK	The number associated with the trunk used to place an outgoing call.
21 (U)	**Additional Call Record**	2	AC	An 'x' in this field indicates that an additional call record related to this call record exists. The additional call record will indicate that this record is the primary record. Not used in Releases 1.0 through 4.x.
22 (V)	**Incoming Trunk Group Access Code**	4	TACI	Reserved. Not supported in this version.
23 (W)	**Tax**	8	Tax	The number of meter pulses associated with this call, indicating the cost of the call. Also called “Advice of Charge.” Used only for international installations.
24 (X)	**Currency**	10	Currency	Currency used to determine the multiplier for this call. Used only for international installations. Default values for supported countries are: **USD** = United States **MARK** = Germany **LIRA** = Italy **YEN** = Japan **CDN** = Canada

Call Detail Record Log field descriptions

Column (Excel)	Field Name	Field Length	CDR Head	Description
25 (Y)	**Multiplier**	4	Mult	Multiplier. The tax amount is multiplied by this value to determine the charge in the state currency. Used only for international installations. Possible values include: **.001** = x1/1000 **.01** = x1/100 **.1** = x1/10 **1** = x1 **10** = x10 **100** = x100 **1000** = x1000
26 (Z)	**TGU**	5	TGU	Time Granularity Units. Unit of time used to charge the call. Used only for international installations. Possible values include: **.001s** = .001 second **.01s** = .01 second **.1s** = .1 second **1s** = 1 second **10s** = 10 seconds **1m** = 1 minute **1h** = 1 hour
27 (AA)	**Primary Call Record ID**	8	Primary	A call record linked to this call record, caused by transferring or parking the call.
28 (AB)	**Extension Record Descriptor**	1	E	Identifies how the remaining record will be interpreted. Valid values are: **0** = No Extension Record **1** = IP Telephony Voice Extension Record; **2** = IP Telephony T.38 Fax Extension Record (*not supported in the current version*) **3** = IP Telephony Video Extension Record (*not supported in the current version*)

IP telephony voice extension record

The Extension Record Descriptor (ERD) determines how the extension record portion of the Call Detail Report should be interpreted. The only valid values for the IP Telephony Extension Record ERD are 0 and 1, which indicate that the extension record should be ignored (0) or analyzed as an IP telephony voice extension record (1). The comma separated value file has fixed length records. If ERD is 0, then applications should skip over the commas and blanks that compose the remainder of the Call Detail Report record.

This extension record contains two symmetrical sections for the origination and the termination sides of the call. Note that the ORIGINATION section corresponds to the DSP codec closest to the Calling Party and that the TERMINATION section corresponds to the DSP codec closest to the Called Party.

The following table describes the fields in the ORIGINATION and TERMINATION sections of the IP Telephony Voice Extension Record. Note that in a Microsoft Excel spreadsheet, columns are indicated by letters, as displayed in the **Column (Excel) Orig/Term** column.

IP telephony voice extension record field descriptions

Column (Excel) Orig/Term	Field Name	Lengt h	Record Heading Orig/Term	Description
29 (AC)/ 43 (AQ)	**Media Endpoint IP Address**	15	OIP/TIP	IP address of the device terminating the RTP stream. If it is an IP phone, this is the IP address of the IP phone. If it is a TDM endpoint (e.g., an analog phone), this is the IP address of the interface being used on the Wave Server. IP address is in `aaa.bbb.ccc.ddd` format (leading zeros are omitted).
30 (AD)/ 44 (AR)	**Media**	2	OM/TM	Specifies the media: **1** = Audio **2** = Fax (future) **3** = Video (future) **4** = Modem Termination (future) **5** = Fax Termination (future)

IP telephony voice extension record field descriptions

Column (Excel) Orig/Term	Field Name	Lengt h	Record Heading Orig/Term	Description
31 (AE)/ 45 (AS)	**Codec**	2	OC/TC	Specifies the codec used on the receiving direction from the endpoint perspective. If Media = 0 (Audio): **0** = G.711 u-law PCM 64kbps **1** = G.711 A-law PCM 64kpbs **2** = G.729A **3** = G.723.1 5.3kbps **4** = G.723.1 6.3kbps If Media = 1 (Fax): **0** = Telogy Fax **1** = T.38 Fax
32 (AF)/ 46 (AT)	**Packet Time**	3	OPT/TPT	Amount of voice information contained per packet (in milliseconds).
33 (AG)/ 47 (AU)	**Bandwidth—Average**	4	OBWA/TBWA	Average bandwidth (in Kbps) used for the call, from the perspective of the receiving direction.
34 (AH)/ 48 (AV)	**Bandwidth—Peak**	4	OBWP/TBWP	Peak bandwidth (in Kbps) used for the call, from the perspective of the receiving direction.
35 (AI)/ 49 (AW)	**Latency—Average**	4	OLA/TLA	The average round trip delay during the call, in milliseconds, calculated per PFC 1889.
36 (AJ)/ 50 (AX)	**Latency—Peak**	4	OLP/TLP	The peak round trip delay during the call, in milliseconds, calculated per PFC 1889.
37 (AK)/ 51 (AY)	**Jitter—Average**	4	OJA/TJA	The average jitter during the call, in milliseconds, calculated per RFC 1889.
38 (AL)/ 52 (AZ)	**Jitter—Peak**	4	OJP/TJP	The peak jitter during the call, in milliseconds, calculated per RFC 1889.
39 (AM)/ 53 (BA)	**Packets Received**	10	OPKTRX/TPKTR X	Count of the total packets received.

IP telephony voice extension record field descriptions

Column (Excel) Orig/Term	Field Name	Length	Record Heading Orig/Term	Description
40 (AN)/ 54 (BB)	**Octets Received**	10	OOCTRX/TOCTRX	Count of the total octets received.
41 (AO)/ 55 (BC)	**Packets Lost—Total**	10	OPKTLT/TPKTLT	Total number of packets lost during the call.
42 (AP)/ 56 (BD)	**Packets Lost—Peak**	10	OPKTLP/TPKTLP	Maximum number of packets lost in any sample period during the call.

The Trunk Statistics report

The Trunk Statistics report provides a generated listing of call statistics for all trunk groups. This report is generated from information gathered by Wave and saved in the Trunk Statistics Log (see “About the Trunk Statistics Log” on page 31-18 for more information).

Caution! *If you change the name of a trunk group and/or the number of channels assigned to a trunk group during the reporting period, you may get unexpected results. For example, if you change the name of a trunk group, you will see one record for each name in the report. If you change the number of channels assigned to a trunk group, you will see two records for that trunk group with the same name but with different data.*

Refer to the following sections for detailed information:

- “Generating the Trunk Statistics report” on page 31-15, provides information about configuring and running the Trunk Statistics Report.
- “Interpreting the Trunk Statistics report” on page 31-17, describes rules, formats and field descriptions for the Trunk Statistics Report.
- “About the Trunk Statistics Log” on page 31-18, describes rules, formats and field descriptions for the Trunk Statistics Log, the raw data from which the report is generated.

Generating the Trunk Statistics report

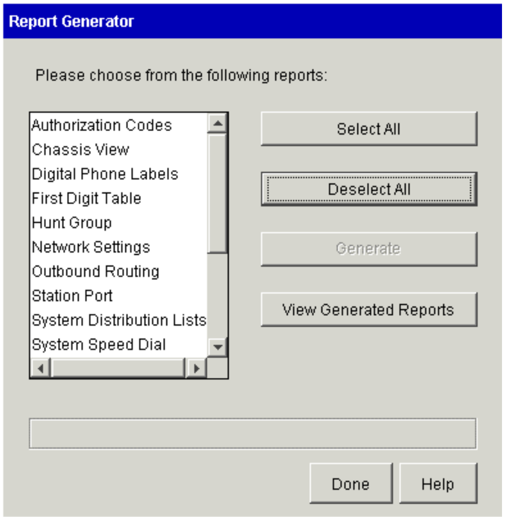
To generate the Trunk Statistics report

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Report Generator icon, located in the General Administration section.

3 Select **Trunk Statistics** from the list of reports, and click **Generate**.

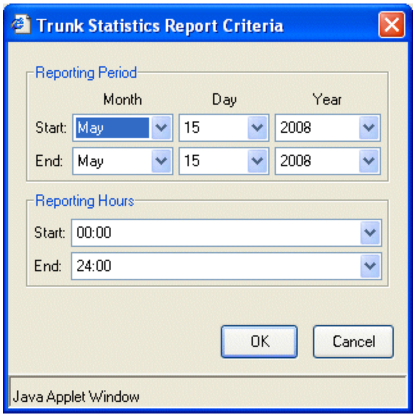


Report Generator

Please choose from the following reports:

- Authorization Codes
- Chassis View
- Digital Phone Labels
- First Digit Table
- Hunt Group
- Network Settings
- Outbound Routing
- Station Port
- System Distribution Lists
- System Speed Dial

4 The Trunk Statistics Report Criteria dialog opens.



Trunk Statistics Report Criteria

Reporting Period

	Month	Day	Year
Start:	May	15	2008
End:	May	15	2008

Reporting Hours

Start: 00:00

End: 24:00

5 Select the starting and ending dates of the period for which you'd like the report, as well as the time range within those dates, and click **OK**.

For example, you might select dates from May 1, 2001 through May 15, 2001 and times from 08:00 to 12:00. The generated report will contain records on May 1 from 08:00 to 12:00, May 2 from 08:00 to 12:00, etc.

The generated report is saved and named TrunkStatistics.html.

Caution! *The previously generated Trunk Statistics report, if there is one, is overwritten.*

6 Click **View the Generated Reports** for a directory listing of all generated reports for Wave.

7 Click TrunkStatistics.html to view the report you generated.

8 Click **Done** to return to the Management Console.

Interpreting the Trunk Statistics report

The following table describes the information contained in the Trunk Statistics report.

Trunk Statistics report columns

Column Name	Description
Trunk Group	Trunk group name.
Size	Total number of analog trunks and digital trunk channels in the group.
Direction	Direction (In, Out, or Both) currently configured (at the time the report is generated) for the trunk group with the given name. Note that if the trunk group direction has changed, only the most recently-configured direction will appear in the report. If the trunk group name has changed or the trunk group has been deleted, “Unknown” will appear in the report.
Busy Hour	Hour (0000, 0100, …, 2300) during which the total usage (inbound and outbound) is greatest. For example, the report would show 1300 as the peak hour if the total use (inbound and outbound) for 13:00, 13:15, 13:30, and 13:45 on all days during the reporting period was greater than the total use for any other hour. If the trunk group was never used, it will report blank for the busy hour.
Calls In	Total number of inbound attempts for this trunk group during the reporting period.
Calls Out	Total number of outbound attempts for this trunk group during the reporting period.
Total Calls	Sum of the computed Calls In and Calls Out values, described above.
Usage In (mins)	Total inbound use in minutes, rounded up to the nearest minute.
Usage Out (mins)	Total outbound use in minutes, rounded up to the nearest minute.
Total Usage (mins)	Sum of the computed Usage In and Usage Out values, described above
% ATB	Percentage of time during which all channels in this trunk group were busy.
% Out Blk	Percentage of outbound calls that were blocked.
Out Svc	Total number of trunks/channels associated with this trunk group that have ever gone out of service during the reporting period.

About the Trunk Statistics Log

Wave ISM gathers trunk and trunk group statistics that are written to the Trunk Statistics Log file every 15 minutes on the hour, quarter hour, half hour, and three-quarter hour. The log file contains the raw data from which the Trunk Statistics Report is generated. The Log is saved in the following location:

```
C:\Inetpub\ftproot\Private\CDR
```

Each Trunk Statistics Log begins with a header. record, described in the following table. Trunk Statistics Log field descriptions for each type of record in the report are enumerated in the tables in subsequent sections.

Trunk Statistics header record field descriptions

Field Name (example)	Description
<HEADER>	Indicates the beginning of the log header.
File ID (TrunkStatistics)	Identifies the type of file.
Version (7)	Specifies the revision of the file format.
Serial Number (123456)	Wave Server serial number entered into the General Settings applet.
Hostname (Wave)	Name of the Wave Server.
IP Address (192.168.205.1)	IP address of the Wave Server.
Start Date (20010430)	Date the file was created.
Start Time (0:00:00)	Time the file was created.
<\HEADER>	Indicates the end of the log header.

Interval record

Each interval posted begins with an Interval record.

Interval record field descriptions

Field Name	Description
I	Identifies this record as an interval record
YYYYMMDD or MMDDYYYY	Date of the start of the interval in either North American or European format
HH:MM	Start time of the interval

Trunk group header record

Each Trunk group record is preceded by a Trunk group header record.

Trunk group header record field descriptions

Field Name	Description
hG	Identifies this record as an trunk group header record
Trunks In Group	Number of trunks in the group at the end of the interval
Group Name	Name of the trunk group
OOS	Number of trunks in a trunk group that were OOS (Out of Service) at the beginning of the interval
Inbound Begin	Number of trunks with incoming calls in progress at the beginning of the interval
Inbound End	Number of trunks with incoming calls in progress at the end of the interval
Inbound Attempts	Number of incoming calls attempted by this trunk group
Inbound Answered	Number of incoming calls by this trunk group that were answered
Inbound Seconds	Total number of seconds that trunks in a trunk group were in the connected state for an incoming, answered call

Trunk group header record field descriptions

Field Name	Description
Outbound Begin	Number of trunks with outgoing calls in progress at the beginning of the interval
Outbound End	Number of trunks with outgoing calls in progress at the end of the interval
Outbound Attempts	Number of outgoing calls attempted by this trunk group
Outbound Answered	Number of outgoing calls by this trunk group that were answered
Outbound Seconds	Total number of seconds that trunks in a trunk group were in the connected state for an outgoing, answered call
Outbound Blocked	Number of outgoing calls that were blocked due to All Trunks Busy (ATB) and/or Out of Service (OOS) Trunks and/or Integrated Services Access (ISA)
ATB Seconds	(All Trunks Busy) Total number of seconds that all trunks in the trunk group are busy and/or out of service

Trunk group record

Each Trunk group record follows the Trunk group header record.

Trunk group record field descriptions

Field Name	Description
G	Identifies this record as an trunk group record
Trunks In Group	Number of trunks in the group at the end of the interval
Group Name	Name of the trunk group
OOS	Number of trunks in a trunk group that were OOS (Out of Service) at the beginning of the interval
Inbound Begin	Number of trunks with incoming calls in progress at the beginning of the interval
Inbound End	Number of trunks with incoming calls in progress at the end of the interval

Trunk group record field descriptions

Field Name	Description
Inbound Attempts	Number of incoming calls attempted by this trunk group
Inbound Answered	Number of incoming calls by this trunk group that were answered
Inbound Seconds	Total number of seconds that trunks in a trunk group were in the connected state for an incoming answered call
Outbound Begin	Number of trunks with outgoing calls in progress at the beginning of the interval
Outbound End	Number of trunks with outgoing calls in progress at the end of the interval
Outbound Attempts	Number of outgoing calls attempted by this trunk group
Outbound Answered	Number of outgoing calls by this trunk group that were answered
Outbound Seconds	Total number of seconds that trunks in a trunk group were in the connected state for an outgoing answered call
Outbound Blocked	Number of outgoing calls that were blocked due to All Trunks Busy (ATB) and/or Out of Service (OOS) Trunks and/or Integrated Services Access (ISA)
ATB Seconds	Total number of seconds that all trunks in the trunk group were busy and/or out of service

Trunk header record

Each Trunk header record follows the Trunk group record. There is one Trunk header record per trunk group.

Trunk header record field descriptions

Field Name	Description
hT	Identifies this record as a trunk header record
Trunk Name	Name of the trunk

Trunk record

Each Trunk record follows the Trunk header record. There is one Trunk record for each trunk in the group.

Trunk record field descriptions

Field Name	Description
T	Identifies this record as an trunk header record
Trunk Name	Name of the trunk
Group Name	Name of the trunk group
OOS	Indicates whether the trunk was OOS (Out of Service) at the beginning of the interval; the value is either 1(TRUE) or 0(FALSE)
Inbound Begin	Indicates whether the trunk had an incoming call in progress at the beginning of the interval
Inbound End	Indicates whether the trunk had an incoming call in progress at the end of the interval
Inbound Attempts	Number of incoming calls attempted by this trunk
Inbound Answered	Number of incoming calls by this trunk that were answered
Inbound Seconds	Total number of seconds that the trunk was in the connected state for an incoming answered call

Trunk record field descriptions

Field Name	Description
Outbound Begin	Indicates whether the trunk had an outgoing call in progress at the beginning of the interval
Outbound End	Indicates whether the trunk had an outgoing call in progress at the end of the interval
Outbound Attempts	Number of outgoing calls attempted by this trunk
Outbound Answered	Number of outgoing calls by this trunk that were answered
Outbound Seconds	Total number of seconds that a trunk was in the connected state for an outgoing answered call

Downloading system reports

You can download Call Detail and Trunk Statistics, and Zone Statistics reports from the Wave Server and save them in another location. All of these are CSV (comma separated values) files that can be easily imported into Microsoft Excel for further processing.

- Call Detail Reports are named “cdryyyymmdd”, for example cdr20080515.csv.
- Trunk Statistics Reports use the format “TrunkStatisticsyyyymmdd.csv”.
- Zone Statistics Reports use the format “ZoneStatisticsyyyymmdd.csv”.

Note: The Call Detail Report (see page 31-2) and the Trunk Statistics Report, (see page 31-14) use the corresponding CSV files listed here as input.

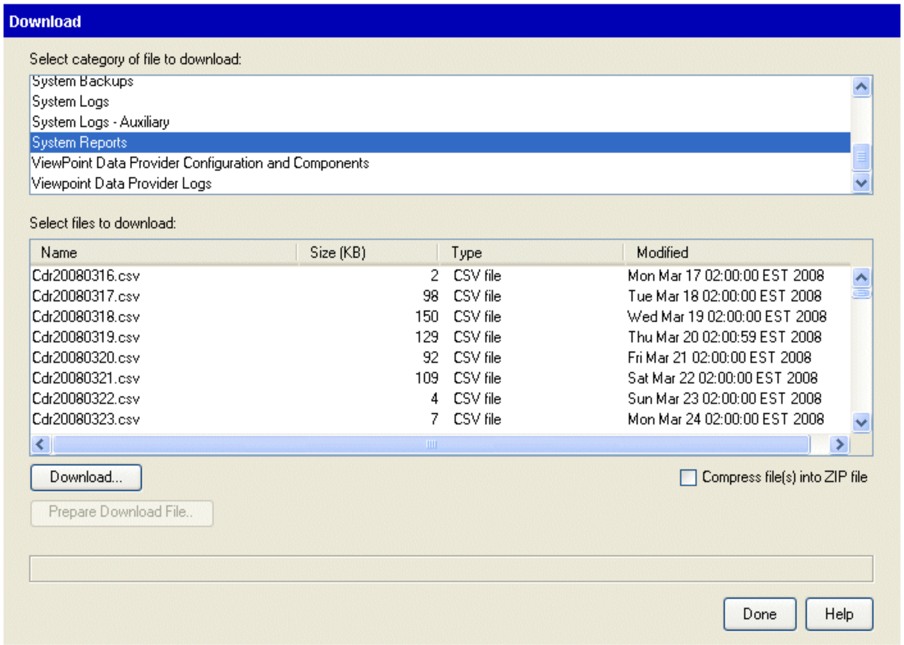
To download reports

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Download icon, located in the General Administration section.

3 From the **Select category of file to download** list box, select **System Reports**. The available reports are displayed.



Download

Select category of file to download:

- System Backups
- System Logs
- System Logs - Auxiliary
- System Reports
- ViewPoint Data Provider Configuration and Components
- Viewpoint Data Provider Logs

Select files to download:

Name	Size (KB)	Type	Modified
Cdr20080316.csv	2	CSV file	Mon Mar 17 02:00:00 EST 2008
Cdr20080317.csv	98	CSV file	Tue Mar 18 02:00:00 EST 2008
Cdr20080318.csv	150	CSV file	Wed Mar 19 02:00:00 EST 2008
Cdr20080319.csv	129	CSV file	Thu Mar 20 02:00:59 EST 2008
Cdr20080320.csv	92	CSV file	Fri Mar 21 02:00:00 EST 2008
Cdr20080321.csv	109	CSV file	Sat Mar 22 02:00:00 EST 2008
Cdr20080322.csv	4	CSV file	Sun Mar 23 02:00:00 EST 2008
Cdr20080323.csv	7	CSV file	Mon Mar 24 02:00:00 EST 2008

☐ Compress file(s) into ZIP file

4 Select one or more files to download. Select contiguous files by holding the Shift key, or select non-contiguous files by holding the Ctrl key.

5 Optionally, click **Compress file(s) into ZIP file**. If you select more than one file, this option is automatically selected.

6 Click **Download**, and save the file.

7 Click **Done** to return to the Management Console.

Using the Report Generator

The Report Generator enables you to generate the following reports from the most recently configured Wave data.

- Authorization Codes
- Chassis View
- First Digit Table
- Hunt Group
- License Status
- Network Settings
- Outbound Routing
- Phone Labels
- Station Port
- System Speed Dial
- Templates
- Trunk Group
- Trunk Statistics
- User Configuration
- User Details
- Zone Bandwidth Statistics
- Zone Paging

All of these reports are HTML files, except for the Phone Labels report, which is a TXT file that can be used with label-making software, as described in “Creating digital phone labels” on page 31-27.

When you generate a report via the Report Generator, the previously-generated version of the report (if one exists) is overwritten.

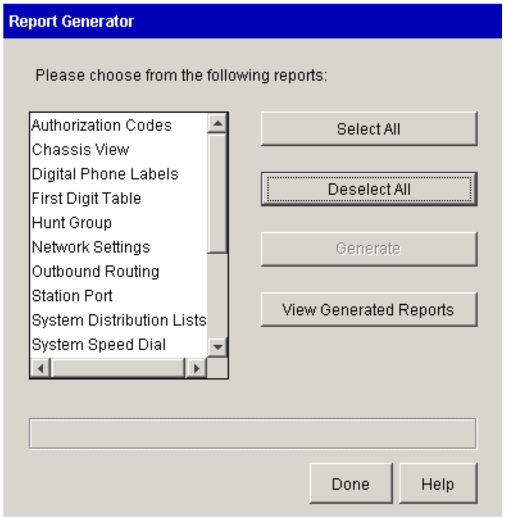
To generate and view a report

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Report Generator icon, located in the General Administration section.

3 Select the desired report from the list, and click **Generate**. To select multiple reports, hold the Ctrl key while selecting them.

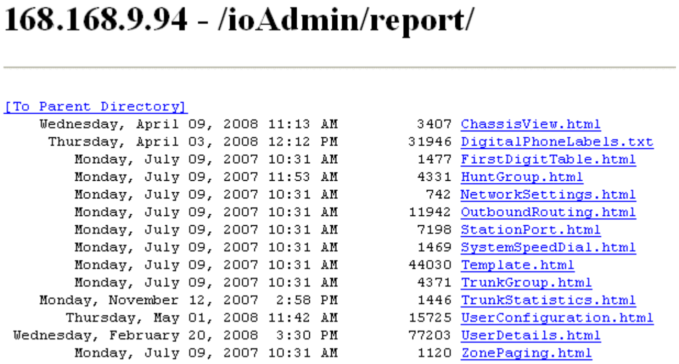


Report Generator

Please choose from the following reports:

Authorization Codes
Chassis View
Digital Phone Labels
First Digit Table
Hunt Group
Network Settings
Outbound Routing
Station Port
System Distribution Lists
System Speed Dial

4 Click **View Generated Reports** to display the date/time stamps for the most recent reports:



168.168.9.94 - /ioAdmin/report/

```
[To Parent Directory]
    Wednesday, April 09, 2008 11:13 AM        3407 ChassisView.html
     Thursday, April 03, 2008 12:12 PM       31946 DigitalPhoneLabels.txt
        Monday, July 09, 2007 10:31 AM        1477 FirstDigitTable.html
        Monday, July 09, 2007 11:53 AM        4331 HuntGroup.html
        Monday, July 09, 2007 10:31 AM         742 NetworkSettings.html
        Monday, July 09, 2007 10:31 AM       11942 OutboundRouting.html
        Monday, July 09, 2007 10:31 AM        7198 StationPort.html
        Monday, July 09, 2007 10:31 AM        1469 SystemSpeedDial.html
        Monday, July 09, 2007 10:31 AM       44030 Template.html
        Monday, July 09, 2007 10:31 AM        4371 TrunkGroup.html
    Monday, November 12, 2007  2:58 PM        1446 TrunkStatistics.html
         Thursday, May 01, 2008 11:42 AM     15725 UserConfiguration.html
 Wednesday, February 20, 2008  3:30 PM       77203 UserDetails.html
        Monday, July 09, 2007 10:31 AM        1120 ZonePaging.html
```

Note: If an error occurs while Wave generates a report, an error.txt file is created and will be displayed here as well.

5. Click a report to view its contents. Generated reports reside on the Wave Server. To copy a report to another location, select **File > Save As** while viewing the report, then select location in the Save In dialog.
6. Click the **Back** button on your browser to return to the list of reports.
7. Close the browser window containing the list of reports to return to the Report Generator applet.
8. Click **Done** to return to the Management Console.

Creating digital phone labels

You can also use the Report Generator applet in conjunction with label-creation software from DESI Telephone Labels to can create professional, printed phone faceplate labels for your digital phones. For information about DESI's label creation software, contact your Wave provider, or go to www.desi.com.

Creating digital phone labels consists generating the Digital Phone Labels data file, and then importing the generated data file into DESI's label-creation software and printing the labels.

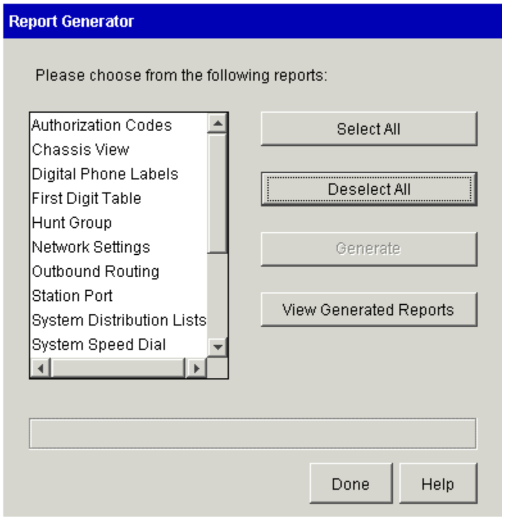
To create digital phone labels

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the Report Generator icon, located in the General Administration section.

3 Select **Digital Phone Labels** from the list of reports, and click **Generate**.



You will see a message when the report generation is complete.

4 Click **View the Generated Reports** for a directory listing of all generated reports for Wave.

5 Click DigitalPhoneLabels.txt to view the data file you generated.

6 Click **Done** to return to the Management Console.

7 See the DESI documentation for information on how to import the file into DESI and print out labels.

Chapter 32

SNMP Agents

CHAPTER CONTENTS

Simple Network Management Protocol (SNMP) can be used to monitor and diagnose the Wave Server, notifying you about any unsolicited events, which are also known as traps. The events detected by SNMP agents are based upon telephony and network standards, such as the IEEE 802.3 Ethernet standard.

All MIBs reside on the Wave Server in the following directory:

```
C:\Program Files\SNMP\MIBs
```

SNMP agent and alarm configuration

Wave provides two panels for configuring and monitoring SNMP:

- **SNMP Configuration panel**. The SNMP Configuration applet lets you configure trap destinations from Wave agents, and permits the following functions:
  - Define valid (up to seven) community strings
  - Identify destination managers who will receive traps (notification about any unsolicited events)
- **SNMP Alarms panel**. The SNMP Alarms applet lets you monitor current and review previous alarms. For further information about using the SNMP Alarms and SNMP Configuration applets, see "Configuring and using SNMP" on page 23-25.

Vertical Communications SNMP agents

The following SNMP agents are supported:

- Environment SNMP agent. See page 32-3.
- Event Log SNMP agent. See page 32-8.
- Interfaces SNMP agent. See page 32-12.
- IP Telephony SNMP agent. See page 32-14.
- ISDN SNMP agent. See page 32-15.
- Repeater Private SNMP agent. See page 32-22.
- Station Private SNMP agent. See page 32-35.
- Self Test Daemon (STD) SNMP agent. See page 32-45.
- T-1 Private SNMP agent. See page 32-52.

Environment SNMP agent

The Environment SNMP agent is responsible for reporting status information about the cooling fans, power supplies, and the fault monitor. This agent also generates appropriate traps to notify Wave of changes in fan status, power supply status, and the status of the fault monitor.

The Environment MIB is structured into the following groups:

Group	Description	Tables contained
Fan Table	Describes status information about all the Wave Server cooling fans.	Fan Table
Power Supply Table	Describes status information about all the Wave Server power supply units.	Power Supply Table
Fault Monitor Group	Contains information about the fault monitor status.	None
Trap Info Group	Contains information about the last fan, power supply, and fault monitor traps.	None
IP Telephony Agent Traps	Generates traps when the status of the fans, power supplies, or fault monitor changes	None

Fan Table

The Fan Table defines objects that describe the status information about each cooling fan in the Wave Server.

Fan Table (Environment SNMP agent)

MIB Variable	Access	Definition	Syntax	Value
fanIndex	R	Numeric index of the cooling fan within the Wave Server.	Integer	
fanOperStatus	R	Specifies the current operational status of the cooling fan. Valid values are: • **Running**. Normal operational status • **Stopped**. Fan is stopped • **Unknown**. Agent is unable to get the status for this fan	Integer	**1** = running **2** = stopped **3** = unknown

Power Supply Table

The Power Supply table defines objects that describe the status information about each power supply unit in the Wave Server.

Power Supply Table (Environment SNMP agent)

MIB Variable	Access	Definition	Syntax	Value
psIndex	R	The numeric index of the power supply unit.	Integer	
psOperStatus	R	Specifies the current operational status of the power supply unit. Valid values are: • **On**. Normal operational status • **Off** • **Unknown**. Agent is unable to get the status for the power supply unit	Integer	**1** = on **2** = off **3** = unknown

Fault Monitor Group

The Fault Monitor Group contains information about the fault monitor status. This group contains just one object, described below.

Fault Monitor group (Environment SNMP agent)

MIB Variable	Access	Definition	Syntax	Value
i**oFaultMonitorStatus**	R	Describes the operational status of the Fault Monitor. Valid values are: • **NotResponding**. Fault monitor is not responding • **ModemFailed**. Fault monitor modem has failed • **OK**. Normal operational state	Integer	**1** = RAMFull **2** = NotResponding **3** = OK **4** = ModemFailed

Trap Info Group

The Trap Info Group contains information about the last fan, power supply, and fault monitor traps.

Trap Info Group (Environment SNMP agent)

MIB Variable	Access	Definition	Syntax	Value
ioLastFanTrap	R	This object describes, in more detail, the last fan trap event that occurred. Since traps for all fans are combined into one trap, this string describes each fan status just after the trap condition.	String	
ioLastPowerSupplyTrap	R	This object describes, in more detail, the last power supply trap event that occurred. Since traps for all power supplies are combined into one trap, this string describes each power supply status just after the trap condition.	String	
ioLastFaultMonitorTrap	R	This object describes, in more detail, the last fault monitor trap event that occurred. Since traps for all fault monitor events are combined into one trap, this string describes each event (RAMFull, NotResponding, or ModemFailed) that caused this trap.	String	

Traps

The Traps agent generates appropriate traps when the status of one or more fans, or the status of one or more power supplies or the status of the fault monitor system change.

Traps (Environment SNMP agent)

Trap #	Trap Name	Description	Pertinent MIB Data
47	ioFanStatus	This notification is sent when one (or more) cooling fans changes state (i.e., it goes from a running state to a stopped state or vice versa). Even if more than one fan changes state, only one trap is sent. Information about the new state of all the fans is sent in the trap data (IOLastFanTrap).	ioLastFanTrap
48	ioPowerSupplyStatus	This notification is sent when one (or more) power supply units changes state (i.e., it goes from an ON state to an OFF state, or vice versa). Even if more than one power supply changes state, only one trap is sent. Information about the new state of all the power supplies is sent in the trap data (IOLastPowerSupplyTrap).	ioLastPowerSupplyTrap
49	ioFaultMonitorStatus	This notification is sent when the following Fault Monitor events occur: • RAM full • Fault Monitor Not Responding • Modem Failed • Information about these events is contained in the trap data (IOLastFaultMonitorTrap).	ioLastFaultMonitorTrap
83	ioSchedulerInfo	This notification is sent whenever an information (including success notification) pertaining to the IOScheduler operation needs to be sent out. Specific information regrading this trap is contained in the Trap data (ioLastIOSchedulerInfoTrap).	ioLastIOSchedulerInfoTrap
84	ioSchedulerWarning	This notification is sent whenever a warning pertaining to the IOScheduler operation occurs. Specific information regarding this trap is contained in the Trap data (ioLastIOSchedulerWarningTrap).	ioLastIOSchedulerWarningTrap

Traps (Environment SNMP agent)

Trap #	Trap Name	Description	Pertinent MIB Data
85	ioSchedulerError	This notification is sent whenever an error pertaining to the IOScheduler operation occurs. Specific information regrading this trap is contained in the Trap data (ioLastIOSchedulerWarningTrap).	ioLastIOSchedulerErrorTrap
92	ioTrapInfoGroup	This notification is sent when one or more temperature sensors measure a temperature outside the normal operating range. Subsequent traps will be generated for each degree of decrease below or increase above the normal operating range. Information about the current state of all the temperature sensors is sent in the Trap Data (ioLastTemperatureOutsideRangeTrap).	ioLastOutsideRangeTemperatureTrap
93	ioTrapInfoGroup	This notification is sent when one or more temperature sensors return to normal operating temperature range. Information about the current state of all the temperature sensors is sent in the Trap Data (ioLastTemperatureInsideRangeTrap).	ioLastInsideRangeTemperatureTrap
94	ioTrapInfoGroup	This notification is sent when one or more DC power supply sensors measure a voltage outside the normal operating range. The power supplies monitored are +2.5, +3.3, +5, +12, and CPU core. Information about the current state of all the DC power supply sensors is sent in the Trap Data (ioLastDCPowerSupplyOutsideRangeTrap).	ioLastOutsideRangeDCPowerSupplyTrap
95	ioTrapInfoGroup	This notification is sent when one or more DC power supply sensors return to normal operating voltage range. Information about the current state of all the power supplies is sent in the Trap Data (ioLastDCPowerSupplyInsideRangeTrap).	ioLastInsideRangeDCPowerSupplyTrap

Event Log SNMP agent

The Event Log SNMP agent is responsible for generating traps when specific Microsoft Windows events are logged. These events can be either application specific, system, or security related. Each of the generated traps contains data specific to the event logged similar to that shown in the event viewer.

The Event Log MIB contains one group.

Group	Description	Tables Contained
Event Log Trap Info Group	Contains more information about the last event log trap that was generated.	None

Event Log Trap Info Group

Event Log Trap Info Group (Event Log SNMP agent)

MIB Variable	Access	Definition	Syntax	Value
lastTrapLogType	R	This object describes the log type of the last event log trap event that occurred. The following are valid values: • **system**. Windows system log • **security**. Windows security log • **application**. Application log • **unknown**. Unknown log	Integer	**1** = system **2** = security **3** = application **4** = unknown
lastTrapEventType	R	This object describes the event type of the last event log trap that occurred. The following are valid values: • **error**. Error events indicate significant problems that the user should know about. Error events usually indicate a loss of functionality or data. For example, if a service cannot be loaded as the Wave Server boots, it can log an error event • **warning**. Warning events indicate problems that are not immediately significant, but that may indicate conditions that could cause future problems. For example, an application can log warning events if disk space is low. • **information**. Information events indicate infrequent but significant successful operations.	Integer	**1**= error **2** = warning **3** = information **4** = audit-success **5** = audit-fail **6** = unknown

Event Log Trap Info Group (Event Log SNMP agent)				
MIB Variable	**Access**	**Definition**	**Syntax**	**Value**
		• **audit-success**. Success audit events are security events that occur when an audited access attempt is successful. For example, a successful log on attempt is a success audit event. • **audit-fail**. Failure audit events are security events that occur when an audited access attempt fails. For example, a failed attempt to open a file is a failure audit event. • **unknown**. Indicates an event type other than those described above.		
lastTrapInfoString	R	This object describes, in more detail, the last event log trap even that occurred. This string contains details of the event like the event id, computer name, time generated, and event specific messages similar to the one seen with the event view application.	String	

Event Log Traps

This agent generates the traps described in the following table, when the appropriate events are logged.

Event Log Traps (Event Log SNMP agent)			
Trap #	**Trap Name**	**Description**	**Pertinent MIB Data**
53	eventLog_FailedToStartSTD	This notification is sent when an attempt to start the Self Start Daemon fails. This event has a Log Type of “application” and an Event Type of “error”.	lastTrapLogType lastTrapEventType lastTrapInfoString
54	eventLog_FailedToStopSTD	This notification is sent when an attempt to stop the Self Start Daemon fails. This event has a Log Type of “application” and an Event Type of “error”.	lastTrapLogType lastTrapEventType lastTrapInfoString

Event Log Traps (Event Log SNMP agent)

Trap #	Trap Name	Description	Pertinent MIB Data
55	eventLog_CannotCreate UserTracePipe	This notification is sent when an attempt to create the User Trace request pipe fails.	lastTrapLogType lastTrapEventType lastTrapInfoString
56	eventLog_CannotConnect UserTracePipe	This notification is sent when an attempt to connect to the User Trace Pipe fails. This event has a Log Type of “application” and an Event Type of “error”.	lastTrapLogType lastTrapEventType lastTrapInfoString
57	eventLog_VoiceMailDiskFull	This notification is sent when the allotted voicemail disk capacity is reached. This event has a Log Type of “application” and an Event Type of “error”.	lastTrapLogType lastTrapEventType lastTrapInfoString
58	eventLog_SystemDiskIsFull	This notification is sent when the specific disk capacity is reached. This event has a Log Type of “system” and an Event Type of “warning”.	lastTrapLogType lastTrapEventType lastTrapInfoString
59	eventLog_SecurityError	This notification is sent when an audited access attempt fails. This event has a Log Type of “security” and an Event Type of “audit-fail”.	lastTrapLogType lastTrapEventType lastTrapInfoString
60	eventLog_SecuritySuccess	This notification is sent when an audited access attempt is successful. This event has a Log Type of “security” and an Event Type of “audit-fail”.	lastTrapLogType lastTrapEventType lastTrapInfoString
61	eventLog_GenericEventLog Trap	This notification is sent whenever an error or warning event, other than the ones described above, is written to the Event Log. More information about this event can be found in the trap data.	lastTrapLogType lastTrapEventType lastTrapInfoString

Interfaces SNMP agent

The Interfaces SNMP agent describes some of the devices installed in the Wave Server and reports their operational status. This agent implements Vertical's private interfaces MIB (interfaces_private.mib), which is based on the Interfaces Table of MIB II.

The devices reported by this agent are:

- T-1 interfaces
- Analog station ports and trunks
- DDS ports
- Repeater Ethernet ports
- Serial interface on T-1 module (reported as Other Interface)

The Interfaces MIB contains one group.

MIB group (Interfaces agent)

Group	Description	Tables contained
Interfaces Group	This group is a place holder for the Interfaces Table, which describes each Wave interface (device) in more detail and also shows its operational status. In addition, this group contains one variable, ifNumber, which basically specifies the number of interfaces displayed in the interfaces group.	Interfaces Table

Interfaces Group

Interfaces Group (Interfaces SNMP agent)				
MIB Variable	**Access**	**Definition**	**Syntax**	**Value**
vifNumber	R	The number of Wave devices (regardless of their current state) present on this system. Size of the integer is 1-’7fffffff’h	Integer	
vifIndex	R	A unique index identifying this interface (device).	Integer	
vifDescr	R	This object describes the interface in more detail. It also specifies the slot number occupied by the interface. Size of the string is 0-255 characters.	String	
vifType	R	This object describes the type of this interface. The type of interface is distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack. The values for these types are taken from the similar table in MIB II. Only the following apply to Wave: • **ds1**. T-1 interface • **other**. All other interfaces	Integer	**1** = other **18** = ds1

vifOperStatus	R	This object describes the current operational status of the interface. The following are valid values:
		• **up**. Normal operation state
		• **down**. Device is not functional
		• **testing**. In a test mode
			Integer	up=1
				down=2
				testing=3

vifSpecific	R	This object refers to the Object Identifier branch of the MIB tree that describes this particular interface in more detail. For example, for T-1 interfaces, ifSpecific should specify Vertical’s T-1 MIB branch, i.e., 1.3.6.1.4.1.2338.3	OID	

IP Telephony SNMP agent

The IP Telephony agent is used to monitor IP Telephony trunks.

IP Telephony Trunk Summary Table

IP Telephony Trunk Summary Table (IP Telephony SNMP agent)

MIB Variable	Access	Definition	Syntax	Value
IpTelTrunkSize	R	Number of trunks.	Integer	
TrunkIndex	R	Trunk number in the trunk table.	Integer	
TrunkState	R	The state of the trunk.	Integer	**0** = not-configured **1** = out_of_service **2** = Initializing **3** = Idle **4** = Outgoing **5** = Incoming **6** = Connected **7** = Disconnecting
CalledParty	R	Number of the called party.	String	
CallingParty	R	Number of the calling party.	String	
RemoteGateway	R	Remote gateway number.	String	
LocalAlarmThreshold	R	Current levels of thresholds reached. It is a bit field indicating the following thresholds: Bit Description • **0** = Jitter • **1** = Network Lost • **2** = Network To Host Errors • **3** = Host To Network Errors • **4** = DSP To Host Errors • **5** = Host To DSP Errors	Integer	
RemoteAlarmThreshold	R	Current levels of thresholds reached. For a description of the bit fields see LocalAlarmThreshold.		

IP Telephony Agent Traps

IP Telephony Agent Traps (IP Telephony SNMP agent)

Trap #	Trap Name	Description	Pertinent MIB Data
64	IpTelReconfigComplete	This notification is sent when the reconfiguration command completes.	IptelTrunkSize
65	IpTelTrunkFailure	This notification is issued when the specified trunk fails	TrunkIndex
66	IpTelTrunkAlarmInfo	Informational alarm associated with some parameter threshold being reached.	TrunkIndex LocalAlarmThreshold RemoteAlarmThreshold

ISDN SNMP agent

The ISDN agent is used to manage Vertical Communication’s ISDN interfaces, including information for managing the Bearer B channels and signaling channels. The ISDN agent is based on Vertical’s private ISDN MIB (isdn_private.mib), using the definitions of SNMP v2 ISDN MIB (RFC 2127) with the syntax changed to reflect SNMP v1. The relative tree structure in this MIB has been retained. In order to manage ISDN interfaces, the following information is necessary:

- Information for managing the physical interface (the T-1 line)

  This information is already provided by the T-1 standard (RFC 1406) and the T-1 private MIB; the respective agents for these MIBs implement the management functionality.

- Information for managing the Bearer B channels

  This information is implemented by this agent.

- Information for managing signaling channels

  This information is implemented by this agent.

The following information is optional:

- Information for managing Terminal Endpoints (TE), for example, the link layer connection to the switch

  Since this is required only if there are non-ISDN endpoints defined for a given D channel, Wave does not implement this.

- Information for managing a list of directory numbers for each signaling channel

  This is not currently implemented by the agent.

Each interface in the system has a unique interface index. In a typical Wave Server, there would be a unique interface index for the following:

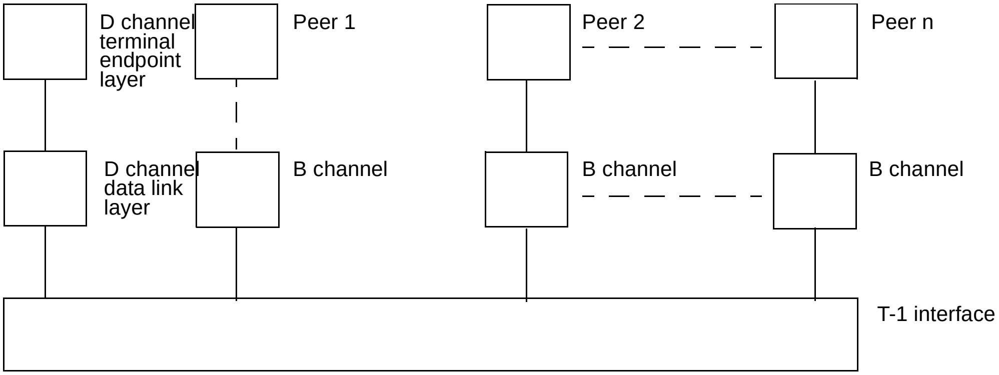
- Each T-1 physical interface of the system
- Each B channel of the system
- The Data link layer (LAPD) of each D channel
- The Network layer (Terminal Endpoint, also called the signaling channel) of each D channel

  Each D channel is subdivided into two layers, the data link and the network layer.

- All other interfaces in the system.

How do all these interfaces fit together? The Interfaces MIB (see “Interfaces SNMP agent” on page 32-12) defines an Interface Table that contains generic descriptive, status, and statistical information about all the interfaces in the system. In a typical management scenario, an alarm received on an interface is reflected by the agent for the interface. The Manager can look up specific alarm information from the interface’s own MIB, note the Interface Index for this interface, and obtain general statistics for this interface (for example, the number of Octets received on this interface, or the bandwidth of this interface) by looking up the Interface Table (corresponding to this index) of the Interfaces MIB.

For the T-1 scenario, the Wave implementation of various layers of interfaces is shown below.



Implementation of the ISDN agent is based on Vertical Communication's private ISDN MIB. The private ISDN MIB (isdn_private.mib) uses the definitions of SNMP version 2 ISDN MIB (RFC 2127), with the syntax changed to reflect SNMP version 1. The relative tree structure in this MIB has been retained.

The ISDN private MIB contains three groups.

Group	Description	Tables contained
Bearer Group	Used to control B (bearer) channels. Contains configuration parameters as well as statistical information related to B channels.	Bearer Table
Signaling Group	Used to control D (Delta) channels. Contains information for ISDN Network layer as well as the Data Link Layer (LAPD) configuration and statistics.	Signaling Table Signaling Stats Table Lapd Table
Directory Group	Used to specify a list of directory numbers for each signaling channel. This group has not been implemented yet.	Not implemented yet

Detailed information about each instrumented variable can be found in the MIB, isdn_private.mib. This agent does not generate any traps.

The Bearer Group

The Bearer Group's sole table, the Bearer Table , has as many entries as there are bearer channels in the whole system (the total of all bearer channels for all devices in the system). Each entry in the table defines configuration as well as statistical parameters required to control one bearer channel.

Examples for these include the bearer channel type (leased vs. dial-up (visdnBearerChannelType)), the bearer channel operator status (idle, connecting, connected, active (visdnBearerOperStatus)). Each entry in this table is indexed by the unique interface index (ifIndex) of the B channel in the system.

Bearer Table (ISDN SNMP Agent, Bearer Group)

MIB Variable	Access	Definition	Syntax	Value
visdnBearerChannelType	R	The B channel type.	Integer	**1** = Dialup **2** = Leased
visdnBearerOperStatus	R	The current call state of the channel.	Integer	**1** = Idle **2** = Connecting **3** = Connected **4** = Active4
visdnBearerChannelNumber	R	The B channel number.	Integer	**1-30**
visdnBearerPeerAddress	R	The ISDN address the current or last call is or was connected to.	String	
visdnBearerPeerSubAddress	R	The ISDN subaddress that the current or last call is or was connected to.	String	
visdnBearerCallOrigin	R	The call origin for the current or last call.	Integer	**1** = Unknown **2** = Originate **3** = Answer **4** = Callback

Bearer Table (ISDN SNMP Agent, Bearer Group)

MIB Variable	Access	Definition	Syntax	Value
visdnBearerInfoType	R	The information transfer capability of the last call. Speech refers to a non-data connection, whereas audio31 and audio7 refers to data mode connections. If there is no call on this interface since system startup, this object has a value of unknown(1).	Integer	**1** = Unknown **2** = Speech **3** = UnrestrictedDigital **4** = UnrestrictedDigital56 **5** = RestrictedDigital **6** = Audio31 **7** = Audio7 **8** = Video **9** = PacketSwitched
visdnBearerMultirate	R	This flag indicates if the current or the last call used multirate.	Boolean	**1** = True **2** = False
visdnBearerCallSetupTime	R	The value of the sysUpTime when the ISDN setup message for the current or last call was sent or received.	Time Stamp	
visdnBearerCallConnectTime	R	The value of the sysUpTime when the ISDN connect message for the current or last call was sent or received.	Time Stamp	
visdnBearerCallChargedUnits	R	The number of charged units for the current or last connection.	Gauge	

The Signaling Group

The Signaling Group is used to control D (delta) channels. The Signaling Group consists of three tables:

- The Signaling Table contains configuration and operational parameters for the Terminal Endpoint layer interface of each D channel.
- The Signaling Stats Table contains statistical information for the same interfaces.
- The LAPD table contains configuration and statistical information for each D channel Data Link layer (LAPD) interfaces of the system.

Note: The Directory Group, used to specify a list of directory numbers for each signaling channel, is not currently implemented.

Signaling Table (ISDN SNMP Agent, Signaling Group)

MIB Variable	Access	Definition	Syntax	Value
visdnSignalingIfIndex	R	The ifIndex value of the interface associated with this signaling channel.	Integer	**1-65535**
visdnSignalingProtocol	R	The particular protocol type supported by the switch providing access to the ISDN network to which this signaling channel is connected.	Isdn Signaling Protocol	**1** = Other **2** = Ds1 **25** = Swissnet3
visdnSignalingCallingAddress	R	The ISDN address to be assigned to this signaling channel.	String	
visdnSignalingSubAddress	R	The ISDN subaddress to be assigned to this signaling channel.	String	
visdnSignalingBchannelCount	R	The total number of B channels managed by this signaling channel.	Integer	**1-65535**
visdnSignalingInfoTrapEnable	R	Indicates whether isdnMibCallInformation traps should be generated for calls on this signaling channel.	Integer	**1** = Enabled **2** = Disabled

Signaling Stats Table (ISDN SNMP Agent, Signaling Group)

MIB Variable	Access	Definition	Syntax	Value
visdnSigStatsInCalls	R	The number of incoming calls on this interface.	Counter	
visdnSigStatsInConnected	R	The number of incoming calls on this interface that were actually connected.	Counter	
visdnSigStatsOutCalls	R	The number of outgoing calls on this interface.	Counter	
visdnSigStatsOutConnected	R	The number of outgoing calls on this interface that were actually connected.	Counter	
visdnSigStatsChargedUnits	R	The number of charged units on this interface since system startup.	Counter	

LAPD Table (ISDN SNMP Agent, Signaling Group)

MIB Variable	Access	Definition	Syntax	Value
visdnLapdPrimaryChannel	R	If true, this D channel is the primary D channel if backup D channel is active. Defaults to True.	Boolean	**1** = True **2** = False
visdnLapdOperStatus	R	The operational status of this interface: • **Inactive**. All layers inactive. • **L1Active**. Layer1 activated, layer 2 datalink not established. • **L2Active**. Layer1 activated, layer 2 datalink established.	Integer	**1** = Inactive **2** = L1Active **3** = L2Active
visdnLapdPeerSabme	R	The number of peer SABME frames received on this interface, for example, the number of peer initiated new connections on this interface.	Counter	
visdnLapdRecvdFrom	R	The number of LAPD FRMR response frames received on this interface, for example, the number of framing errors on this interface.	Counter	

Repeater Private SNMP agent

The Repeater Private SNMP agent monitors and manages all repeater devices within the Wave system. The Wave implementation is based on Vertical Communication’s private repeater MIB (repeater_private.mib). The private MIB module combines the syntax of SNMP version 1 definition for IEEE 802.3 repeaters (RFC 1516) with the additional features defined in the SNMP version 2 (RFC 2108). The structure of the private MIB closely follows that of the definition in RFC 2108, with the relative tree structure of the variables unchanged.

Note: For descriptions of each statistical variable in the repeater hub agent tables, see ASN.1 definitions in the Vertical Communications private repeater MIB (repeater_private.mib).

The Repeater Private MIB contains four groups.

Group	Description	Tables contained
Basic Package Group	Describes objects that are applicable to all repeaters within the system: status, parameter, and control objects for each repeater within the managed system, for the port groups within the system, and for the individual ports themselves.	Group Table Port Table Info Table
Monitor Group	Contains definitions for monitoring statistics for each repeater within the system as well as for individual ports within the system.	Monitor Port Table Monitor 100Port Table Monitor Repeater Table Monitor 100Repeater Table
Address Tracking Group	Includes objects for tracking the MAC addresses of the DTEs attached to the ports within the system. This is an optional group and has not been implemented.	None
TopN Group	Includes objects for tracking the ports with the most activity within the system. This is an optional group and has not been implemented in the current version.	None

Basic Package Group

The Group Table contains status information about each group of ports within the system, such as the Operation Status of the group (operational, malfunctioning, notPresent) (vrptrGroupOperStatus), the port capacity of this group (vrptrGroupPortCapacity).

Group Table (Repeater Private SNMP Agent, Basic Package Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrGroupIndex	R	Identifies the group within the system for which this entry contains information.	Integer	**1-2147483647**
vrptrGroupObjectID	R	The vendor's authoritative identification of the group.	OID	
vrptrGroupOperStatus	R	An object that indicates the operational status of the group. A status of notPresent (4) indicates that the group is temporarily or permanently, physically and/or logically, not a part of the repeater. It is an implementation-specific matter as to whether the agent effectively removes notPresent entries from the table.	Integer	**1** = other, **2** = operational **3** = malfunctioning **4** = notPresent **5** = underTest **6** = resetInProgress
vrptrGroupPortCapacity	R	The vrptrGroupPortCapacity is the number of ports that can be contained within the group. Within each group, the ports are uniquely numbered in the range from 1 to vrptrGroupPortCapacity.	Integer	**1-2147483647**
vrptrGroupSlotNumber	R	The slot number in which this repeater device resides.	Integer	**1-18**
vrptrGroupBroadcast domainNumber	R	This object indicates the repeater's broadcast domain. This value will be 0 if the broadcast domain number is unknown.	Integer	**1-18**

Group Table (Repeater Private SNMP Agent, Basic Package Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrGroupNetworkAdapterNumber	R	This object indicates the identification number of the Wave network adapter associated with the repeater, if any. This value will be 0 if the repeated domain number is unassociated or unknown.	Integer	**1-255**
vrptrGroupLedStatus	R	This object indicates the status of the card LEDs. The Led status is shown for any card that has an Ethernet interface. A status of unknown (1) indicates that the LED status is not available from the hardware. All 10Mb cards will return a value of unknown for its LEDs since the LED information for 10Mb cards are not available. A status of none (2) indicates neither the green nor the red LED is ON. A status of greenRed (5) indicates that both the green and the red LEDs are ON.	Integer	**1** = unknown **2** = none **3** = green **4** = red **5** = greenRed

The Port Table contains status information about each managed repeater port in the system, for each repeater hub in the system. Examples of these are the administrative status of the port (enabled, disabled (vrptrPortAdminStatus)), the operational status of the port (operational, notPresent (vrptrPortOperStatus)).

Port Table (Repeater Private SNMP Agent, Basic Package Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrPortGroupIndex	R	Identifies the group containing the port for which this entry contains information.	Integer	**1-2147483647**
vrptrPortIndex	R	Identifies the port within the group for which this entry contains information. This identifies the port independently from the repeater it may be attached to.	Integer	**1-2147483647**
vrptrPortAdminStatus	R/W	Setting this object to disabled(2) disables the port.	Integer	**1** = Enabled **2** = Disabled

Port Table (Repeater Private SNMP Agent, Basic Package Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrPortAutoPartitionState	R	This flag indicates whether the port is currently partitioned by the repeater's auto-partition protection.	Integer	**1** = notAutoPartitioned **2** = autoPartitioned
vrptrPortOperStatus	R	This object indicates the port's operational status.	Integer	**1** = Operational **2** = NotOperational **3** = NotPresent
vrptrPortRptrId	R	Identifies the repeater to which this port belongs.	Integer	**1-2147483647**
vrptrPortLinkState	R	Specifies whether there is a link on this port or not.	Integer	**1** = link **2** = noLink
vrptrPortSpeed	R	Specifies the Ethernet speed of this particular port.	Integer	**1** = unknown **2** = 10Mbps **3** = 100Mbps
vrptrPortSpeedSelect	R	Indicates the selection used by the port for negotiating the Ethernet speed. If automatic is selected, the highest supported speed will be negotiated.	Integer	**1** = speed-select-auto **2** = speed-select-10 **3** = speed-select-100
vrptrPortDuplex	R	Indicates the duplex of the Ethernet port	Integer	**1** = unknown **2** = half **3** = full
vrptrPortDuplexSelect	R	Indicates the selection used by the port for negotiating the Ethernet duplex. If automatic is selected, the best supported duplex will be negotiated.	Integer	**1** = duplex-select-auto **2** = duplex-select-half **3** = duplex-select-full
vrptrPortPolarity	R	Indicates the polarity of the Ethernet cable. If the polarity is crossed, the repeater may compensate for it, but it indicates a wiring problem with the attached Ethernet device.	Integer	**1** = unknown **2** = straight **3** = crossed

The Info Table (see below) contains status information about each repeater hub within the system.

In Wave implementation, a Group is the same as a separate repeater, so the information in the Info Table and the Group Table complement each other. These tables have been kept separate in keeping with the MIB structure in RFC 2108.

Info Table (Repeater Private SNMP Agent, Basic Package Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrInfoId	R	Identifies the repeater for which this entry contains information.	Integer	**1-2147483647**
vrptrInfoRptrType	R	Identifies the CSMA/CD repeater type. The value of 5 (tenMbOrOnehundredMb) is a Vertical Communications extension specifying 10/100 Mb repeater which contains mixed 10 Mb and 100 Mb ports.	Integer	1 = Other 2 = tenMb 3 = onehundredMbClassI 4 = onehundredMbClassII 5 = tenMbOrOnehundredMb
vrptrInfoOperStatus	R	Indicates the operational state of the repeater.	Integer	**1** = Other **2** = OK **3** = Failure
vrptrInfoReset	R	Setting this object to reset (**2**) causes a transition to the START state. Setting to noReset (**1**) has no effect.	Integer	**1** = NoReset **2** = Reset

Info Table (Repeater Private SNMP Agent, Basic Package Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrInfoPartitionedPorts	R	Returns the number of ports in the repeater that are in the autoPartitioned state.	Integer	**0-24**
vrptrInfoLastChange	R	The values of syUpTime when any of the following conditions occurred: • Agent cold or warm started • This instance of repeater was created • A change in rptrInfoOperStatus • Ports were added or removed • Any of the counters in this repeater had a discontinuity	Integer	

Monitor Group

The Monitor Port Table contains performance and error statistics for each port in the system.

Monitor Port Table (Repeater Private SNMP Agent, Monitor Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPortGroupIndex	R	Identifies the group containing the port for which this entry contains information.	Integer	**1-2147483647**
vrptrMonitorPortIndex	R	Identifies the port within the group for which this entry contains information.	Integer	**1-2147483647**
vrptrMonitorPortReadableFrames	R	The number of frames of valid frame length that have been received on this port.	Integer	
vrptrMonitorPortReadableOctets	R	The number of octets contained in valid frames that have been received on this port.	Integer	**-1** = notSupported **0** = supported

Monitor Port Table (Repeater Private SNMP Agent, Monitor Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPortFCSErrors	R	The number of frames with FCS error signal asserted on this port.	Integer	**-1** = notSupported **0** = supported
vrptrMonitorPortAlignmentErrors	R	The number of frames with FCS and Framing error signals asserted.	Integer	**-1** = notSupported **0** = supported
vrptrMonitorPortFrameTooLongs	R	The number of frames with OctetCount greater than maxFrameSize.	Integer	**-1** = notSupported **0** = supported
vrptrMonitorPortShortEvents	R	This counter is incremented by one for each CarrierEvent on this port with ActivityDuration less than ShortEventMaxTime.	Integer	
vrptrMonitorPortRunts	R	Usually indicates collision fragments.	Integer	**-1** = notSupported **0** = supported
vrptrMonitorPortCollisions	R	This counter is incremented by one for any CarrierEvent signal on any port for which the CollisionEvent signal on this port is asserted.	Integer	**-1** = notSupported **0** = supported
vrptrMonitorPortLateEvents	R	This counter is incremented by one for each CarrierEvent on this port in which the CllIn(X) variable transitions to the value SQE.	Integer	
vrptrMonitorPortVeryLongEvents	R	This counter is incremented by one for each CarrierEvent on this port whose ActivityDuration is greater than the MAU Jabber Lockup Protection timer TW3.	Integer	
vrptrMonitorPortDataRate Mismatches	R	Data Rate mismatches as per the definitions in the MIB (repeater_private.mib).	Integer	**-1** = notSupported **0** = supported

Monitor Port Table (Repeater Private SNMP Agent, Monitor Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPortAutoPartitions	R	This counter is incremented by one each time the repeater has automatically partitioned this port.	Integer	
vrptrMonitorPortTotalErrors	R	The total number of errors which have occurred on this port.	Integer	
vrptrMonitorPortLastChange	R	The value of syUpTime when any of the following conditions occurred: • Agent cold or warm started. • The row for the port was created. • Any of the counters in this repeater had a discontinuity.	Integer	
vrptrMonitorPortSentFrames	R	This object is the number of frames of valid frame length that have been sent on this port. This counter is incremented by one for each frame sent on this port whose OctetCount is greater than or equal to minFrameSize and less than or equal to maxFrameSize.	Integer	

Monitor Port Table (Repeater Private SNMP Agent, Monitor Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPortSentOctets	R	This object is the number of octets contained in valid frames that have been sent on this port. This counter is incremented by one for each frame sent on this port which has been determined to be a readable frame (i.e., including FCS octets but excluding framing bits and dribble bits). For ports receiving traffic at a maximum rate in a 100Mb/s repeater, this counter can roll over in less than six minutes. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information a management station is advised to also poll the rptrMonitorPortUpper32SentOctets object, or to use the 64-bit counter defined by rptrMonitorPortHCReadableOctets instead of the two 32-bit counters.	Integer	
vrptrMonitorPortDroppedFrames	R	This counter is incremented by one for every time the switch dropped a frame due to a buffer full event.	Integer	
vrptrMonitorPortOtherErrors	R	This counter is incremented by one every time the repeater detects an error that is not reported in any other error counter. The frame may or may not be lost due to the error.	Integer	

Monitor 100 Port Table

The Monitor 100 Port table lists additional performance and error statistics for 100Mb/s ports, above and beyond those parameters that apply to both 10 and 100 Mbps ports. Entries exist only for ports attached to 100 Mbps repeaters.

Monitor 100 Port Table (Repeater Private SNMP Agent, Monitor Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPort Isolates	R	This counter is incremented by one each time that the repeater port automatically isolates as a consequence of false carrier events.	Counter	
vrptrMonitorPort SymbolErrors	R	This counter is incremented by one each time when valid length packet was received at the port and there was at least one occurrence of an invalid data symbol. This can increment only once per valid carrier event.	Counter	
vrptrMonitorPortUpper32Octets	R	This object is the number of octets contained in valid frames that have been received on this port, module 2**32. That is, it contains the upper 32 bits of a 53-bit octets counter, of which the lower 32 bits are contained in the rptrMonitorPortReadableOctets object. This two-counter mechanism is provided for those network management protocols that do not support 64-bit counters (e.g., SNMP V1) and are used to manage a repeater type of 100Mb/s.	Counter	
vrptrMonitorPortUpper32SentOctets	R	This object is the number of octets contained in valid frames that have been sent on this port, modulo 2**32. That is, it contains the upper 32 bits of a 64-bit octets counter, of which the lower 32 bits are contained in the rptrMonitorPortSentOctets object.	Counter	

Monitor Repeater Table

The Monitor Repeater Table shows performance and error statistics for 10 MB repeaters within the system.

Monitor Repeater Table (Repeater Private SNMP Agent, Monitor Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrMonTxCollisions	R	This counter is incremented every time the repeater state machine enters the TRANSMIT COLLISION state from any state other than ONE PORT LEFT.	Integer	**-1** = notSupported **0** = supported
vrptrMonTotalFrames	R	The number of frames of valid frame length that have been received on this port for which the FCSError and CollisionEvent signals were not asserted.	Counter	
vrptrMonTotalErrors	R	The total number of errors which have occurred on all the ports of this repeater.	Counter	
vrptrMonTotalOctets	R	The total number of octets contained in valid frames that have been received on ports in this repeater.	Integer	**-1** = notSupported **0** = supported
vrptrMon100Table	NA	A table of additional information about each 100 Mb/s repeater, augmenting the entries in the rptrMonTable. Entries exist in this table only for 100 Mb/s repeaters.	Sequence of VRptrMon100Entry	
vrptrMon100Entry	NA	An entry in the table, containing information about a single 100 Mbps repeater.	VRptrMon100Entry	

Monitor Repeater Table (Repeater Private SNMP Agent, Monitor Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrMonUpper32TotalOctets	R	The total number of octets contained in the valid frames that have been received on the ports in this repeater, modulo 2**32. That is, it contains the upper 32 bits of a 64-bit counter, of which the lower 32 bits are contained in the rptrMonTotalOctets object. If an implementation cannot obtain a count of octets as seen by the repeater itself, the 64-bit value may be the summation of the values of the rptrMonitorPortReadableOctets counters combined with the corresponding rptrMonitorPortUpper32Octets counters for all the ports in the repeater.	Counter	
vrptrMonHCTotalOctets	R	The total number of octets contained in the valid frames that have been received on the ports in this group. If an implementation cannot obtain a count of octets as seen by the repeater itself, this counter may be the summation of the values of the rptrMonitorPortReadableOctets counters for all of the ports in the group.		

Monitor Repeater 100 Table

The Monitor Repeater 100 table lists additional information about each 100 Mb repeater, augmenting the entries in the rptrMonTable. Entries exist in this table only for 100 Mb repeaters.

Monitor Repeater 100 Table (Repeater Private SNMP Agent, Monitor Group)

MIB Variable	Access	Definition	Syntax	Value
vrptrMonUpper32TotalOctets	R	The total number of octets contained in the valid frames that have been received on the ports in this repeater, modulo 2**32. That is, it contains the upper 32 bits of a 64-bit counter, of which the lower 32 bits are contained in the rptrMonTotalOctets object. If an implementation cannot obtain a count of octets as seen by the repeater itself, the 64-bit value may be the summation of the values of the rptrMonitorPortReadableOctets counters combined with the corresponding rptrMonitorPortUpper32Octets counters for all the ports in the repeater.	Counter	
vrptrMonHCTotalOctets	R	The total number of octets contained in the valid frames that have been received on the ports in this group. If an implementation cannot obtain a count of octets as seen by the repeater itself, this counter may be the summation of the values of the rptrMonitorPortReadableOctets counters for all of the ports in the group.	Counter	

Station Private SNMP agent

The Station Private SNMP agent is used to monitor, configure and control all station devices within the Wave system. Additionally, this agent can be used to configure the First Digit Table (which contains settings for each digit that is dialed as the first digit), as well as to configure an interface with an external voicemail system.

The Station Private MIB contains four groups:

- **Common Group**. Contains status and configuration information that are common to all Station devices within the system.
- **Station Card Group**. Contains status, control, and configuration information about all cards containing station devices within the system. This information is arranged into three tables: the Card Table, the Device Table, and the Channel Table.
- **Digit Table Group**. Contains configuration information of digits that can be dialed. Currently this group contains just one table, the First Digit Table, which contains settings for each digit (0-9) dialed as the first digit.
- **External Voicemail System Group**. Contains configuration information used to interface with an external voicemail system. Currently there is one subgroup: the ATT_System_25 subgroup.

Common Group

Common Group (Station Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vStationFirstDigitTimeout	R	Specifies the maximum number of seconds to wait for the first digit.	Integer	
vStationDigitTimeout	R	Specifies the maximum number of seconds to wait between digits.	Integer	
vStationOffHookTimeout	R	Specifies the maximum number of seconds to wait for the user to hang up after a call disconnects or the user executes an invalid operation. Howler tone is applied at time-out.	Integer	

Common Group (Station Private SNMP Agent)				
MIB Variable	**Access**	**Definition**	**Syntax**	**Value**
vStationNumStationCards	R	Specifies the number of station cards installed in the system.	Integer	
vStationExternalDialDigit	R	Identifies the starting digit for making an external call.	String	SIZE (**0-1**)

Station Card Group

The Station Card Group consists of Card Table, Device Table, and Channel Table.

Card Table

Card Table (Station Private SNMP Agent, Station Card Group)				
MIB Variable	**Access**	**Definition**	**Syntax**	**Value**
vStationCardSlotNumber	R	Physical slot in the system in which the card is installed.	Integer	**1-14**
vStationCardType	R	The Vertical Communications card type.	Integer	**0** = card-type-NOT-CONFIGURED **2** = card-type-24-CHANNEL STATION **3** = card-type-BRIDGE1
vStationCardIOPort Address	R	The ISA bus base address for the card.	Integer	**0-’7fffffff’h**
vStationCardState	R	The current status of the card.	Integer	**0** = Disabled **1** = Enabled **255** = Removed
vStationCardErrorLED	R	All Vertical Communications cards have an Error LED and a Ready LED. The combined value of these LEDs are as follows:	Integer	**0-1**

Card Table (Station Private SNMP Agent, Station Card Group)

MIB Variable	Access	Definition			Syntax	Value
		Error	**Ready**	**Value Definition**		
		off	off	(0 0) invalid		
		on	off	(1 0) powering up		
		on	on	(1 1) initializing		
		off	on	(0 1) normal		
vStationCardReadyLED	R	See vStationCardErrorLED.			Integer	**0-1**

Device Table

Device Table (Station Private SNMP Agent, Station Card Group)

MIB Variable	Access	Definition	Syntax	Value
vStationDeviceSlotNumber	R	Physical slot in the system in which the card containing the device is installed.	Integer	**0-255**
vStationDeviceDeviceNumber	R	The logical device number for this station device in its card.	Integer	**0-255**
vStationDeviceIfIndex	R	The Interface index for this device. The value for this object correlates to the IfIndex found in MIB-II	Integer	**1-’7fffffff’h**
vStationDeviceBaseIOAddress	R	The ISA bus base address for this card.	Integer	**0-’7fffffff’h**
vStationDeviceEnabled	R	Setting this variable to Disabled will disable this particular station device.	Integer	**0** = Disabled **1** = Enabled
vStationDeviceInterrupt	R	Interrupt Request level for this card.	Integer	**1-2147483647**
vStationDeviceNumChannels	R	The ISA bus address for this card.	Integer	**1-’7fffffff**’h
vStationDeviceMVIPStartingChannel	R	Vertical Communications card revision level.	Integer	**0-255**

Device Table (Station Private SNMP Agent, Station Card Group)

MIB Variable	Access	Definition	Syntax	Value
vStationDeviceMVIP Stream	R	Vertical Communications card identification number.	Integer	**0-255**
vStationDeviceType	R	Specifies the type of device: **0** = undefined **8** = station	Integer	**0** = devUndef **8** = devSation
vStationDeviceChange Pending	R	Interrupt Request level for this card/trunk.		**0-'7fffffff'**h

Channel Table

Channel Table (Station Private SNMP Agent, Station Card Group)

MIB Variable	Access	Definition	Syntax	Value
vStationChannelIndex	R	This is the logical channel number of the channel within its station device. For 12 channel station devices, it is between 1 and 12. For 24 channel station devices, it is between 1 and 24.	Integer	**1-24**
vStationChannelSlot Number	R	The logical number of the slot in which the card containing the channel is located.	Integer	**0-255**
vStationChannelDevice Number	R	The logical device number of the device containing this channel within its slot, that is, vstationDeviceDeviceNumber.	Integer	**0-255**
vStationChannelChannel Type	R	The Channel Type.	Integer	**1** = loopStart **2** = groundStart
vStationChannelMWI Type	R	Defines the type of message waiting indicator.	Integer	**0** = notConfigured **1** = stutter **2** = lamp

Channel Table (Station Private SNMP Agent, Station Card Group)

MIB Variable	Access	Definition	Syntax	Value
vStationChannel OperationMode	R	Defines the operation mode of the channel.	Integer	**0** = notConfigured **1** = station **2** = voiceMail **3** = notConfigured
vStationChannelState	R	Indicates the operational state of this channel.	Integer	**0** = disabled **1** = enabled
vStationChannelType	R	The phone type for this particular channel.	Integer	**1** = basic **2** = callerID **3** = enhanced-Call Waiting

Channel Table (Station Private SNMP Agent, Station Card Group)

MIB Variable	Access	Definition	Syntax	Value
vStationChannelCallState	R	Indicates the phone call state of this channel. **0** = call-state-VOID **1** = call-state-IDLE **2** = call-state-DIALING **3** = call-state-COLLECT-FIRST-DIGIT **4** = call-state-COLLECT-DIGITS **5** = call-state-CALL-OFFERED **6** = call-state-PROCEEDING **7** = call-state-RINGING **8** = call-state-ALERTING **9** = call-state-CONNECTED **10** = call-state-DISCONNECTING **11** = call-state-FAILED **12** = call-state-UNAVAILABLE **13** = call-state-OFFHOOK **14** = call-state-INITIALIZE **15** = call-state-INITIALIZING **16** = call-state-DIAL-REQUEST **17** = call-state-HELD **18** = call-state-FEATURE-INVOKED **19** = call-state-OFFHOOK-IDLE **20** = call-state-OFFHOOK-ACTIVE **21** = call-state-OUT-OF-SERVICE **22** - call-state-OUTPULSING	Integer	**0-22**
vStationChannelCalled PartyNumber	R	The called party’s number, either an internal extension or external phone number.	String	**0-32**

Channel Table (Station Private SNMP Agent, Station Card Group)				
MIB Variable	**Access**	**Definition**	**Syntax**	**Value**
vstationChannelCalling PartyNumber	R	The calling party's number, either an internal extension or external phone number.	String	**0-32**
vStationChannelChange Pending	R	Indicates that a change to the channel values have been made to the registry. The interpretation of the values are: 1=The change is made to the registry, but not yet incorporated in the device. 0=The device changes the value to 0 from 1, after it incorporates the value from the registry.	Integer	**0-1**

Digit Table Group

The Digit Table Group consists of the First Digit Table.

First Digit Table

First Digit Table (Station Private SNMP Agent, Digit Table Group)				
MIB Variable	**Access**	**Definition**	**Syntax**	**Value**
vStationDigitIndex	R	The index to an entry in the First Digit Table.	Integer	**1-10**
vStationDigitString	R	The first digit string.	String	SIZE (**0-1**)

First Digit Table (Station Private SNMP Agent, Digit Table Group)

MIB Variable	Access	Definition	Syntax	Value
vStationDigitCallType	R/W	Type of call generated by this digit. Valid values are: **0** = fc-VOID **1** = fc-HOLD-CALL **2** = fc-PARK-CALL **3** = fc-STATION-CALL **4** = fc-LONG-DISTANCE-CALL **5** = fc-INTERNATIONAL-CALL **6** = fc-LOCAL-CALL **7** = fc-OPERATOR-CALL **8** = fc-RECEPTIONIST-CALL **9** = fc-CAMP-ON-CALL	Integer	**0-9**
vStationDigitMoreDigits	R/W	The number of additional digits to collect after the matched digits.	Integer	**0-32**
vStationDigitStripDigits	R/W	The number of leading digits to strip from the digits collected before they are reported up to the connection manager.	Integer	**0-32**

External Voicemail System Group

This group contains configuration information used to interface with an external voicemail system. This group is subdivided into subgroups depending on the type of voicemail system used. The External Voicemail System Group consists of the ATT System 25 Subgroup.

ATT System 25 Subgroup

The ATT System 25 subgroup contains the Voicemail Call Handle table.

Voicemail Call Handle Table (Station Private SNMP Agent, ATT System 25 Subgroup

MIB Variable	Access	Definition	Synta x	Value
vStationMWILampON	R	Command expected from the external voicemail system to switch on the station's message waiting indicator lamp.	String	SIZE (**0-10**)
vStationMWILampOFF	R	Command expected from the external voicemail system to switch off the station's message waiting indicator lamp.	String	SIZE (**0-10**)
vStationVMCallHandle Type	R	Indicates the type of access to voicemail port made. **1** = An external caller coming directly into the voicemail port. **2** = An external caller calling an extension, and forwarded to the voicemail port. **3** = An internal caller coming directly into the voicemail port. **4** = An internal caller calling an extension, and forwarded to the voicemail port.	Integer	**1** = directExternal **2** = forwardExternal **3** = directInternal **4** = forwardInternal
vStationVMCallHandle Opcode	R	The Opcode string for this operation.	Octet String	SIZE (0-32)
vStationVMCallHandle SRCNumber	R	The source number format string. It contains a C type '%s' where the source number would be filled in.	Octet String	SIZE (0-32)
vStationVMCallHandle DSTNumber	R	The destination number format string. It contains a C type '%s' where the destination number would be filled in.	Octet String	SIZE (0-32)

Traps

Traps (Station Private SNMP Agent)

Trap #	Trap Name	Description	Pertinent MIB Data
12	vStationCannotPlayTone	This notification is sent when the specific channel cannot play a tone.	vStationChannelSlotNumber vStationChannelDeviceNumber vStationChannelIndex
13	vStationCannotCancelTone	This notification is sent when the specific channel cannot cancel a tone.	vStationChannelSlotNumber vStationChannelDeviceNumber vStationChannelIndex
14	vStationCannotAttachDigit Collector	This notification is sent when the specific channel cannot release digits collected.	vStationChannelSlotNumber vStationChannelDeviceNumber vStationChannelIndex
15	vStationCannotReleaseDigit Collector	This notification is sent when the specific channel cannot release digits collected.	vStationChannelSlotNumber vStationChannelDeviceNumber vStationChannelIndex
16	vStationRECONFIG-COMPLETE	This notification is sent when the specific station device successfully reads and incorporates the values from the registry.	vStationChannelSlotNumber vStationChannelDeviceNumber
17	vStationRECONFIG-ERROR	This notification is sent when the specific station device fails to incorporate the values read from the registry.	vStationChannelSlotNumber vStationChannelDeviceNumber

Self Test Daemon (STD) SNMP agent

The Self Test Daemon SNMP agent is responsible for showing status and control information for Vertical Communications' Self Test Daemon (STD). The Self Test Daemon is responsible for starting and monitoring each Wave component (executable, service, and drivers). The status of each component (started, stopped, paused, disabled, etc.) as well as the status of the system as a whole is made available.

In addition, since the Self Test Daemon controls the Upgrade and Restore process, this agent generates appropriate traps to notify the various stages of the Upgrade and the Restore (in case the upgrade is unsuccessful) process. For detailed information about each of these traps, see "STD SNMP Agent Traps" on page 32-48.

The STD MIB contains two groups.

Group	Description	Tables Contained
System Group	Describes status information about the Wave system as a whole.	None.
Component Group	Contains status information of each component (executable, service, or driver) within the system.	STDComponentTable

System Group

The System Group contains just two objects.

System Group (STD SNMP Agent)

MIB Variable	Access	Definition	Synta x	Value
sysOperStatus	R	Specifies the current operational status of the Wave Server. Valid values are: • running. Normal operational status, all components are up and running • startUpInProgress. STD is starting up the system • upgradeInProgress. STD is attempting to upgrade the system • restoreInProgress. STD is attempting to restore the system from a previous installation, after an upgrade attempted failed • error. One or more components failed to start. More information can be found from the components table	Integer	**0** = running **2** = startUpInProgress **3** = upgradeInProgress **4** = restoreInProgress error=5
sysCurrentVersion	R	Specifies the current Wave version of the system.	String	

Component Group

The Component Group contains just one table, the Component table. The Component table defines objects that describe the status information about each component in the system. The following table describes each of these objects.

Component Group (STD SNMP Agent, Component Group)

MIB Variable	Access	Definition	Syntax	Value
compIndex	R	Specifies the numeric index of this component	Integer	
compName	R	Specifies the name of this component	String	
compType	R	Specifies the component type.	Integer	**1** = type-driver **16** = type-service **2000** = type-executable **2001** = type-non-vni-driver **2002** = type-non-vni-service **2003** = type-non-vni-executable

compInstallStatus	R	Describes the installation status of this component.	Integer	uninstalled=100
				installed=1

compOperStatus	R	Describes the operational status of this component.	Integer	**1** = stopped **2** = start-pending **3** = stop-pending **4** = running **5** = continue-pending **6** = pause-pending **7** = paused **8** = unknown **1025** = disabled
compEnabled	R	Determines whether this component is enabled or disabled	Integer	**100** = enabled **1** = disabled
compLastStart	R	Specifies the date-time stamp when this component was last restarted	String	

STD SNMP Agent Traps

The Self Test Daemon (STD) SNMP agent generates appropriate traps when a trappable condition occurs. Traps generated by this agent fall into two categories:

- Traps that are related to the components controlled by STD (like ComponentFailedToStart, ComponentRestartComplete, etc.)
- Traps that are related to the Upgrade and Restart process. Trap are generated at appropriate stages of the entire upgrade/restore process so that any connected manager will be able to trace the entire sequence of the Upgrade and Restore process (in case the upgrade is unsuccessful). The stages of an upgrade and restore process and the traps generated during this stage are described in the following table.

Upgrade and Restore Stages (STD SNMP Agent)	
An upgrade request comes in	• CAB file is pushed • stdUpgradeStarted trap is sent
Unpacking of the CAB file is done	• stdUnpackingFiles trap is sent • Multiple stdUpgradeInProgress traps are sent during this period
Unpacking is complete	• stdUnpackingComplete trap is sent
A system reboot is done	• stdRebootingMachine trap is sent
Upgrade is applied	• stdUpgradeBeingApplied trap is sent • Multiple stdUpgradeInProgress traps are sent during this period
System is rebooted again	• stdRebootingMachine trap is sent
All components are started	• stdVerifyingSystem trap is sent
• If success	• stdUpgradeComplete trap is sent, all is well
• If failed	• stdUpgradeError trap is sent • A restore operation is attempted
Restore is attempted	• stdRestoreStarted trap is sent • Multiple stdRestoreInProgress traps are sent at this point
A system reboot is done	• stdRebootingMachine trap is sent
All components are started	• stdVerifyingSystem trap is sent

Upgrade and Restore Stages (STD SNMP Agent)	
• If success	• stdRestoreComplete trap is sent
• If failed	• stdRestoreError trap is sent • STD quits

Traps (STD SNMP Agent)			
26	stdCompFailedToStart	This trap is generated when a component fails to start during initial start up. The Self Test Daemon will attempt to restart this component five times (once each minute), after which it gives up.	sysCurrentVersion compName
27	stdCompAttemptRestart	This trap is generated when the Self Test Daemon attempts to restart a component.	sysCurrentVersion compName
28	stdCompFailedToReStart	This trap is generated when a n attempt to restart a component fails.	sysCurrentVersion compName
29	stdCompRestartComplete	This trap is generated when a component is restarted successfully.	sysCurrentVersion compName
30	stdUpgradeStarted	This trap is generated when an Wave upgrade is started.	sysCurrentVersion
31	stdUnpackingFiles	This trap is generated when unpacking of the generated CAB files starts	sysCurrentVersion
32	stdUnpackingComplete	This trap is generated when unpacking of the upgraded CAB file is complete.	sysCurrentVersion
33	stdUpgradeBeingApplied	This trap is generated when an Wave upgrade is about to be applied. This is done after the CAB file is unpacked and a system reboot is done.	sysCurrentVersion
34	stdUpgradeInProgress	This trap is generated when an Wave upgrade process is under way.	sysCurrentVersion
35	stdUpgradeComplete	This trap is generated when an Wave upgrade is successfully completed.	sysCurrentVersion
36	stdUpgradeError	This trap is generated when an Wave upgrade attempt fails. A Restore operation would be done immediately.	sysCurrentVersion

Traps (STD SNMP Agent)

37	stdRestoreStarted	This trap is generated when a previous version of Wave is about to be restored. A Restore operation is typically carried out after a failed upgrade attempt.	sysCurrentVersion
38	stdRestoreInProgress	This trap is generated when a previous version of Wave is being restored.	sysCurrentVersion
39	stdRestoreComplete	This trap is generated when a previous version of Wave is successfully restored	sysCurrentVersion
40	stdRestoreError	This trap is generated when a Restore to a previous version of Wave fails. STD normally quits at this point.	sysCurrentVersion
41	stdRebootingMachine	This trap is generated just before an Wave reboot is done, typically due to an upgrade/restore request.	sysCurrentVersion
42	stdVerifyingSystem	This trap is generated when the Wave system is brought up (all components are started) after an Upgrade or a Restore process.	sysCurrentVersion
50	stdIOUptoDate	This notification is sent when an upgrade attempt is aborted because the current version of the Wave software is later than the upgrade version.	sysCurrentVersion
51	stdBadCABFile	This notification is sent when an upgrade attempt is aborted because of a bad CAB file.	sysCurrentVersion
52	stdNotEnoughDiskSpace	This notification is sent when an upgrade attempt is aborted because there is not enough disk space on the machine.	sysCurrentVersion

Traps (STD SNMP Agent)			
63	stdIoNotOperational	This notification is sent under any of the following conditions: • Before attempting to start the components, FBS checks to ensure the minimum configuration is present in the Wave Server. Currently this means that an RSC card must be present in the Wave Server. If this check fails, FBS will not attempt to start any of the components and sends the trap. • When FBS attempts to start all components and a critical component fails to start, rendering the Wave Server non-operational, FBS sends the trap. • After an upgrade is performed and deemed unsuccessful, FBS will attempt to restore to the previous working version of the system software. In case this process fail, FBS sends the trap.	sysCurrentVersion compName
67	stdPrerequisiteMissing	This notification is sent when an upgrade attempt is done on an Wave system that does not contain the prerequisite software version to do the upgrade.	sysCurrentVersion compName
70	stdPLDFailed	Integrated Services Card Firmware upgrade failed.	sysCurrentVersion compName
88	stdLowDiskSpace	This notification is sent periodically whenever there is low disk space on the machine.	sysCurrentVersion
89	stdHardDiskError	This notification is sent if there is any disk errors found during the daily disk checking.	sysCurrentVersion, compName
90	stdEventLogError	This notification is sent when there are event mining dll matching errors found in the event log.	sysCurrentVersion, compName

T-1 Private SNMP agent

The T-1 Private SNMP agent is based on the VerticalCommunications' private extension MIB to RFC 1406, and is used to manage the T-1 physical interface, analog channels, and the Integrated Services Card trunk interface. This extension MIB defines additional variables which facilitate the management of the Vertical Wave T-1 modules.

The Private MIB (t1_private.mib) is organized into three tables:

- Card Table. Contains status information about each Wave T-1 module. There is one row in the table for each module.
- Trunk Table. Defines configuration and status information for each trunk on each T-1 module. There is one entry in this table for each trunk of each module.
- Channel Table. Contains generic configuration, status and statistical information about each channel of each trunk.

Card Table

Each entry in the Card Table describes the read-only status of a T-1 module in the Wave system, for example, the module type (T-1 module, analog trunk module, Integrated Services Card (vdsx1CardType)), the module slot number (vdsx1CardSlotNumber), the module ISA address (vdsx1CardISAAddress).

Card Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1cardSlotNumber	R	Physical slot in the system in which the card is installed	Integer	1-14
vdsx1cardType	R	Vertical's card type	Integer	**1** = cardTYPE-DUAL-T1 **3** = cardTYPE-8-TRUNK **4** = cardTYPE-RESOURCE1 **13** = cardTYPE-8-CHANNEL-DID **100** = cardTYPE-NOT-CONFIGURED
vdsx1cardDescr	R	Vertical card identification number	Integer	**0-255**

Card Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1cardRevision	R	Vertical card revision level	Integer	**0-255**
vdsx1cardDriverVersion	R	Vertical card driver version	Integer	**0-255**
vdsx1cardIOPortAddress	R	The ISA bus address for this card	Integer	**0-'7fffffff'**h
vdsx1cardErrorLED		The ERROR LED state on this card: The combined values of the ERROR LED and the READY LED are: Error Ready Definition OFF OFF Invalid state ON OFF Just after power up ON ON Software initialization OFF ON Normal operation	Integer	**0** = OFF **1** = ON
vdsx1cardReadyLED	R	The READY LED state on this card. See above description for various combined values of READY and ERROR LEDs.	Integer	**0** = OFF **1** = ON

Trunk Table

Each entry in the following table contains configuration information about each trunk in each module of the system, such as the type of Trunk (T-1, as well as Common Channel Signaling (CCS) vs. Channel Associated Signaling (CAS) (vdsx1TrunkType). In addition, this table describes various status information relating to this trunk, such as the channel count for this trunk (vdsx1channelCount). Each entry in the trunk table is indexed by the interface number of the T-1 device within the system.

Trunk Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1TrunkIfIndex	R	The ifIndex (dsx1IfIndex) of this DS1 interface.	Integer	**1-’7fffffff’**h
vdsx1TrunkIndex	R	The index into the number of trunks associated with the card containing this trunk.	Integer	**1-’7fffffff’**h
vdsx1TrunkIdentifier	R	The value of the dsx1CircuitIdentifier from the Configuration Table of the T-1 standard MIB.	String	
vdsx1TrunkSlotNumber	R	The logical number of the card containing this trunk.	Integer	**0-255**
vdsx1TrunkDeviceNumber	R	The value for this object is the logical device number of this trunk within its slot. This number may be used to identify this device in the registry.	Integer	**0-255**
vdsx1TrunkInterrupt	R	Interrupt Request level for this card/trunk. NOTE: all trunks in the same card have the same IRQ.	Integer	**1-2147483647**

Trunk Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1TrunkEnabled	R	Setting this variable to Deactivated will disable the trunk.	Integer	**1** = vdsx1TrunkActivated **2** = vdsx1TrunkNotConfigured **100** = vdsx1TrunkDeactivated
vdsx1TrunkMasterPriority	R	Designates the priority for selecting which trunk is to drive the MVIP clock, for example, which trunk drives the master timing system. The values must be different for each trunk in the system.	Integer	**1** = primary **2** = secondary **100** = notUsed
vdsx1TrunkStream	R	The MVIP stream for this trunk.	Integer	**0-7**
vdsx1TrunkStartingChannel	R	The starting MVIP channel for this trunk within its MVIP stream. If CardType is DTM or WAN1, this value is 0; if CardType is CO-POTS, this value is 16 or 24.	Integer	**0** = DTM or WAN1 **16** or **24** = CO-POTS
vdsx1TrunkType	R	The trunk type for this trunk: defines T-1 and Common Channel Signaling (CCS) vs. Channel Associated Signaling (CAS). All applicable device types are listed here.	Integer	**1** = dev-t1CAS **2** = dev-t1CCS **7** = dev-coPOTS **16** = dev-CSU-DSU **100** = dev-undef

Trunk Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1TrunkIsdnSignalingProtocol	R	Defines the switch type for the Isdn protocol stack. • **not-applicable** = not a supported configuration • **invalid** = not in range • **ess4** = USA/AT&T 4ESS • **ess5** = USA/AT&T 5ESS • **dms100** = USA/Northern Telecom DMS100 • **ni2** = USA/National ISDN 2 (BRI, PRI) • **dms100s100** = NT DMS-100 switch/S-100	Integer	**0** = not-applicable **1** = invalid **5** = ess4 **6** = ess5 **7** = dms100 **10** = ni2 **263** = dms100s100
vdsx1TrunkLineCoding	R	Line coding for Trunk. T-1 trunk.	Integer	**2** = B8ZS **5** = AMI
vdsx1TrunkFraming	R	Defines framing for trunk. T-1 trunk can be either ESF (2) or D4 (3).	Integer	**1** = other **2** = ESF **3** = D4
vdsx1TrunkNumberOfChannels	R	The maximum number of channels to be initiated for this trunk: 0-24 for T-1, 0-8 for CO POTS.	Integer	**0-24**
vdsx1TrunkLineBuildOut	R	Defines the line build out option.	Integer	**1** = buildOut-minus7point5 dB **2** = buildOut-minus15dB **3** = buildOut-minus22point5dB **100** = buildOut-0dB

Trunk Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1TrunkLoopback	R	This variable represents the loopback configuration of the DS1 interface.	Integer	**1** = vdsx1NoLoop **2** = vdsx1PayloadLoop **3** = vdsx1LineLoop **4** = vdsx1OtherLoop
vdsx1TrunkRedLED	R	Specifies the RED LED status of this trunk.	Integer	**0** = OFF **1** = ON
vdsx1TrunkYellowLED	R	Specifies the YELLOW LED status of this trunk.	Integer	**0** = OFF **1** = ON
vdsx1TrunkChangePending	R	Indicates that a change to the device values have been made to the registry. The interpretation of the values are: **1** = change made to the registry, but not incorporated in the device yet. **0** = the device changes the value to 0 from 1, after it incorporates the value from registry.	Integer	**0-1**
vdsx1TrunkLOSThreshold	R	Loss of Signal Threshold in volts. The value is indirectly defined by vdsx1TrunkLoopLength.	Integer	**0** = lOS1point36 **1** = lOS1point04 **2** = lOS0point84 **3** = lOS0point62 **4** = lOS0point43 **5** = lOS0point32 **6** = lOS0point22 **7** = lOS-NOT-IN-USE
vdsx1TrunkTransmit PulseMask	R	Transmit Pulse Mask. Its value is indirectly defined by vdsx1TrunkLoopLength.	Integer	**1-16777215**
vdsx1TrunkReceive Equalizer	R	Receive Equalizer. Its value is indirectly defined by vdsx1TrunkLoopLength.	Integer	**0** = FALSE **1** = TRUE

Channel Table

Each entry in the following table contains configurable parameters for each channel of each trunk, such as the type of channel (wink start, ground start, clear channel, B channel, D channel(vdsx1ChannelType)), channel enabled status (vdsx1ChannelActivated).

All configurable parameters are written to the registry on each successful SET operation (an operation to set the configuration parameters over SNMP), and the driver reconfigures the device appropriately.

Channel Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1channelIndex	R	The logical channel number of the channel within its trunk.	Integer	**1-32**
vdsx1channelTrunk Index	R	The index of the trunk relative to its card.	Integer	**0-255**
vdsx1channelSlot Number	R	The slot number of the card to which the trunk containing this channel belongs (vdsx1cardSlotNumber).	Integer	**0-255**
vdsx1channelTrunk DeviceNumber	R	The value for this object is the logical device number of the trunk containing this channel within its slot, for example, vdsx1TrunkDeviceNumber.	Integer	**0-255**
vdsx1channelEnabled	R	Setting this variable to Deactivated will disable the channel.	Integer	**1** = vdsx1channelActivated **100** = vdsx1channelDeactivated

Channel Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1channelType	R	The channel type: - vdsx1channelTypeUnknown. Unknown type - vdsx1channelTypeWink. Ear and Mouth (E & M) start - vdsx1channelTypeGs. Ground start digital trunk - vdsx1channelTypeClear. Nailed up clear channel for data - vdsx1channelTypeAnalogImm. Analog trunk, immediate start - vdsx1channelTypeBChan. PRI B channel on T-1 - vdsx1channelTypeDChan. PRI D channel on T-1 - vdsx1channelTypeAnalogDt. Analog Trunk, dialtone start - vdsx1channelTypeAnalogGs. Analog Trunk, ground start - vdsx1channelTypeDDS. DDS channel (56K or 64K) - vdsx1channelTypeAnalogDID. Analog channel, DID wink	Integer	**2** = vdsx1channelTypeWink **5** = vdsx1channelTypeGS **6** = vdsx1channelTypeClear **7** = vdsx1channelType AnalogImm **8** = vdsx1channelTypeBChan **9** = vdsx1channelTypeDChan **11** = vdsx1channelType AnalogDt **12** = vdsx1channelType AnalogGs **13** = vdsx1channelTypeDDS **14** = vdsx1channelType AnalogDID **100** = vdsx1channelType Unknown

Channel Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1channelState	R	Indicates current state of this channel. • **OOS** = Out Of Service • **Idle** = Idle • **InCall** = Inbound call • **OutCall** = Outbound call • **Offline** = Off line • **Other** = Other state • **Data** = Data • **Error** = Error • **FeRinging** = Ringing far end • **NeRinging** = Incoming ringing • **DigitSend** = Sending digits • **DigitRcv** = Receiving digits • **IncallEst** = Incall established • **OutcallEst** = Outcall established • **IncallClear** = Incall clearing • **OutcallClear** = Outcall clearing	Integer	**1** = channelStateOOS **2** = channelStateIdle **3** = channelStateInCall **4** = channelStateOutCall **5** = channelStateOffline **6** = channelStateOther **7** = channelStateData **8** = channelStateError **9** = channelStateFeRinging **10** = channelStateNeRinging **11** = channelStateDigitSend **12** = channelStateDigitRcv **13** = channelStateIncallEst **14** = channelStateOutcallEst **15** = channelStateIncallClear **16** = channelStateOutcallClear
vdsx1channel CallerID	R	The callerID of an incoming caller, if available. If the callerID is not available, then it will have a length of zero.	String	
vdsx1channel ExternalAddress	R	The far end number of a connected call on this channel. If the number is not available, then it will have a length of zero.	String	
vdsx1channel ExternalSubAddress	R	The far end sub address of a connected call on this channel. If this is not available, then it will have a length of zero.	String	
vdsx1channelLocal Address	R	The local number of a connected call on this channel. If the number is not available, then it will have a length of zero.	String	

Channel Table (T-1 Private SNMP Agent)

MIB Variable	Access	Definition	Syntax	Value
vdsx1channelLocal SubAddress	R	The local sub address of a connected call on this channel. If the number is not available, then it will have a length of zero	String	
vdsx1channelChange Pending	R	Indicates that a change to the channel values have been made to the registry. The interpretation of the values is: • **1** = change made to the registry, but not incorporated in the device yet. • **0** = the device changes the value to 0 from 1, after it incorporates the value from registry.	Integer	**0-1**

T-1 Private Agent Traps

The T-1 private agent also generates the traps and trap notifications to any connected manager under the line error conditions described in the following table.

.

Traps (T-1 Private SNMP Agent)

1	vdsx1TrunkRedClear	This notification is sent when the specific trunk RED alarm condition clears.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
2	vdsx1TrunkRed	This notification is sent when the specific trunk goes into the RED alarm situation. Red alarm condition signifies LOS (Loss of Signal) failure, i.e. the receiver sees no positive or negative pulses.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
3	vdsx1TrunkYellowClear	This notification is sent when the specific trunk YELLOW alarm condition clears.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex

Traps (T-1 Private SNMP Agent)

4	vdsx1TrunkYellow	This trap is generated when the specific trunk goes into a YELLOW alarm condition (for example, Loss of Frame condition).	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
5	vdsx1TrunkBlueClear	This notification is sent when the specific trunk BLUE alarm condition clears.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
6	vdsx1TrunkBlue	This trap is generated when the specified trunk goes into a BLUE alarm condition (for example, Alarm Indication Signal, AIS, meaning the source is sending an unframed stream of one's).	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
7	vdsx1TrunkReconfigComplete	This trap is generated when the trunk has been reconfigured by the driver in response to a SET operation.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
8	vdsx1TrunkReconfigError	This trap is generated if the driver is unable to reconfigure the trunk (because of an illegal value or state on a SET operation).	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
43	vdsx1TrunkLoopbackPayloadOn	This notification is sent when the specific trunk enters a payload loopback state. Payload loopback means that the received signal at this interface is looped through the device. Typically the received signal is looped back for re-transmission after it has passed through the device's framing function.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
44	vdsx1TrunkLoopbackPayloadOff	This notification is sent when the specific trunk moves from a payload loopback state to a non-loopback state.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex

Traps (T-1 Private SNMP Agent)			
45	vdsx1TrunkLoopbackLineOn	This notification is sent when the specific trunk enters a line loopback state. Under this state the received signal at this interface does not go through the device (minimum penetration) but is looped back out.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
46	vdsx1TrunkLoopbackLineOff	This notification is sent when the specific trunk goes out of a Line Looped state	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
86	vdsx1TrunkAnalogDisconnect	This notification is sent when the specific analog trunk is disconnected.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
87	vdsx1TrunkAnalogConnect	This notification is sent when the specific analog trunk is connected	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
91	vdsx1EnterChannelErrorState	This notification is sent when unexpected signaling is detected on a T-1 channel or analog trunk. While in this state, the T-1 channel or analog trunk is out of service.	vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex vdsx1TrunkIdentifier

Chapter 33

System Locale Settings

Chapter Contents

The Wave Server system locale sets the default phone display language, the call numbering plan, tone sets, and other system settings associated with the locale that you specify. Depending on the specified locale, SIP phone softkeys will be displayed in English, French, German, Russian, or Spanish.

This chapter describes how to change the default Wave Server system locale and provides information about the advanced locale settings found in the General Settings applet.

Caution! *The default advanced settings for a locale should work for you unless you have a unique environment. These are expert settings that should not be modified unless you are instructed to do so by your Vertical Technical Support representative.*

Setting and viewing system locale settings

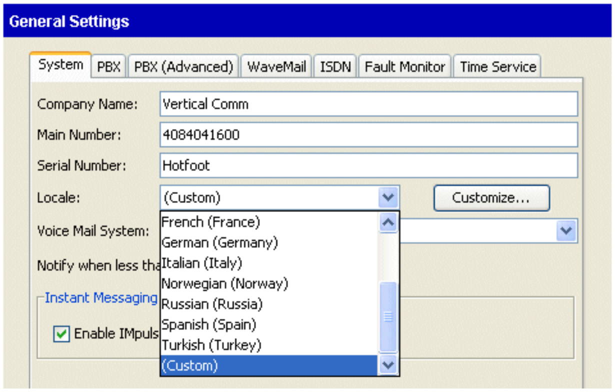
To access the System Locale settings

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 On the System tab, if the **Locale** is correct for your system, go to step 4. If not, select your locale from the drop-down list.



General Settings

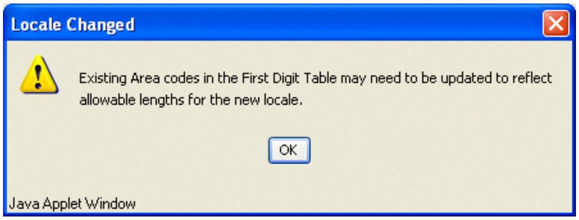
Company Name: Vertical Comm

Main Number: 4084041600

Serial Number: Hotfoot

Locale: (Custom)

When you change the locale, you are reminded that you may need to update any area codes that you have already defined in the First Digit Table to reflect new area code requirements for the selected locale.



Locale Changed

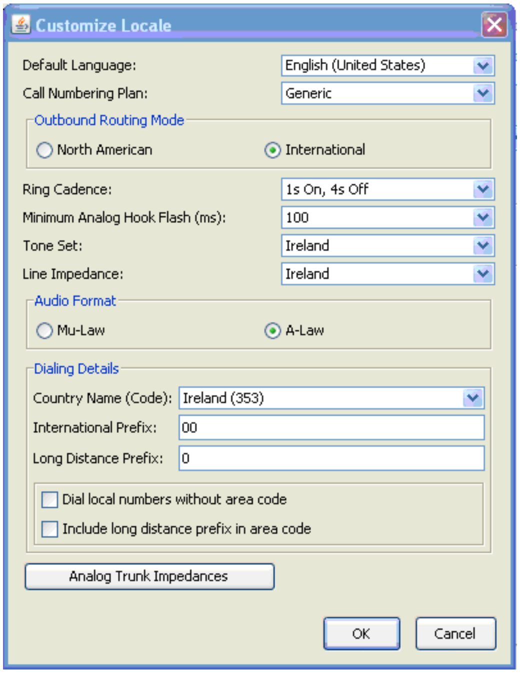
Existing Area codes in the First Digit Table may need to be updated to reflect allowable lengths for the new locale.

For more about editing the First Digit Table, see “Setting the home area code” on page 7-5.

Click **OK** to continue.

4 Click **Customize** to review the default advanced locale settings or to change the settings if you have a unique environment.

The Customize Locale dialog opens.



Customize Locale

Default Language: English (United States)

Call Numbering Plan: Generic

Outbound Routing Mode

○ North American ● International

Ring Cadence: 1s On, 4s Off

Minimum Analog Hook Flash (ms): 100

Tone Set: Ireland

Line Impedance: Ireland

Audio Format

○ Mu-Law ● A-Law

Dialing Details

Country Name (Code): Ireland (353)

International Prefix: 00

Long Distance Prefix: 0

□ Dial local numbers without area code

□ Include long distance prefix in area code

Selecting a locale, specifies the following information:

- **Default Language**. Specifies the default language used on the displays of digital phones, which you may override in when you configure users on the system. If the language has not been set in the User Configuration, Mailbox Configuration, or AutoAttendant Scheduling panels, theWave system will default to the language specified in this field.
- **Call Numbering Plan**. Specifies the format of phone numbers. Depending on the locale you choose, the selected call numbering plan may affect the settings in the Dialing group box on the PBX (Advanced) tab of the General Settings applet.

- **Outbound Routing Mode**. Determines how outbound calls are processed. Select **North American** or **International**.
- **Ring Cadence**. Specifies the duration of each ring and the pause between rings.
- **Minimum Analog Hook Flash**. Specifies in milliseconds the minimum time an analog phone user must hold down the switch hook to indicate a flash.
- **Tone Set**. Affects the tones (dial tone, busy tone, and so forth) that users will hear.
- **Line Impedance**. Sets the line impedance of analog trunks to match your locale's default line impedance.
- **Audio Format**. Sets the mode for analog-to-digital conversion on the Wave Server.
  - **Mu-Law** (the default) is the most common audio format used in North America.
  - **A-Law** is the most common format outside of North America.
- **Dialing Details**. The default values for the following settings may need to be changed depending on the dialing details for your site:
  - **Country Name (Code)**. Select one of the available country names and codes from the drop-down list..
  - **International Prefix**. Enter a numeric international prefix of 1-3 digits. Note that this field cannot be blank.
  - **Long Distance Prefix**. Enter a numeric long distance prefix of 1-3 digits.
  - **Dial local numbers without area code.**
  - **Include long distance prefix in area code.**

5. Click **OK** to return to the General Setting applet System tab.
6. Click **Apply** to save your changes.
7. Click **Done** to return to the Management Console.

Chapter 34

Trunk Settings

Chapter Contents

Line Build Out settings

Line Build Out is a means of simulating additional cable length between a T-1 trunk's transmitter and the far-end receiver. This is done in case the signal being transmitted is too strong. When the phone company deploys T-1 lines, each cable runs for 6000 feet before going into a repeater to boost the T-1's signal strength. When the T-1 line reaches its final destination, the final span will generally not be exactly 6000 feet. Instead, the span length will be somewhere between 0 and 6000 feet and average 3000 feet. If the final span is much less than the average, the final repeater's receiver will be much too close to the customer's transmitter. The customer's transmitter signal will be too strong for the repeater to handle.

There are three FCC sanctioned signal levels that the customer can be asked to provide. They are as follows:

- **0 dB**. No artificial cable and therefore no reduction in signal strength
- **-7.5 dB**. Puts the signal at 50 percent power
- **-15 dB**. Puts the signal at 25 percent power

The customer provisioning letter will state what the Line Build Out (LBO) should be set at. If the provisioning letter does not give an LBO value, then use the 0 dB default.

Wave also provides a -22.5 dB LBO value (12.5 percent power). This is not sanctioned by the FCC and should never be used with the PSTN. However, for private networks where the far end is only a few feet away, this might be useful.

The default, 0 dB, is the most common signal level for connection to the carrier. If line build out is set incorrectly, the carrier may detect errors, prompting an SNMP yellow alarm and a yellow LED on the T-1 module. If you see such indicators and cannot determine another cause, try changing the Line Build Out setting.

Note: The yellow alarm will occur only in case of extreme errors, such as one in 100 bits being bad.

Customizing transmit and receive signal settings

In the event that the standard Line Build Out settings are not correct for your T-1 configuration, you can customize the following Line Build Out settings. For configuration instructions, see “Configuring digital trunk card or module settings” on page 5-23.

Caution! *Do not modify line build out settings unless you work with your T-1 provider to determine appropriate settings.*

Note: If you find a “canned” cable length that works well, these settings will be grayed out and ignored. If you specify that you are using a Custom Cable, these settings will be used.

- Enable Receive Equalizer

  This setting determines whether automatic receive equalization is enabled or not. If this is enabled, the Wave T-1 framer chip automatically and intelligently boosts the signal coming in to the optimal level for pulse detection. This is called automatic equalization. In this mode, the Wave system can accommodate an incoming signal strength range between -36 and -0 dB.

  If the Enable Receive Equalizer check box is disabled, a fixed (non-intelligent) 6 dB boost is added to the receive signal. If this box is disabled, the Receive Input Threshold list box is then enabled.

- Specify the Receive Input Threshold level

  You enable this when you disable the Enable Receive Equalizer check box. When automatic receive equalization is turned off, the framer chip recovers signals by comparing directly to a Receive Input Threshold. If the signal is lower than the threshold, the chip senses a 0. If the signal is higher than the threshold, the chip senses a 1. If the signal is exactly the same as the threshold, the result is unpredictable.

  1.36 volts is the default threshold level. T-1 signals generally range between 0 and 3 volts in amplitude. However, if a signal is extremely weak, you can set the receive threshold to as little as .22 volts.

  Setting the Receive Input Threshold attempts to reduce the input threshold value to accommodate a small input signal.

  Note that there are two problems with disabling the automatic equalizer. First is that the Wave system cannot adjust for dynamic changes in the signal strength of the T-1 line with the fixed boost given by the T-1 framer chip. Second, you must try to guess what the optimal input threshold level is. Generally, the automatic equalizer can determine the optimal input signal level better than you can guess the input threshold level.

- Edit the Transmit Pulse Mask

  This field allows you to input raw data to directly determine four points on the shape template of the T-1 pulse that is transmitted. Any changes to this field can easily cause the far-end to be unable to receive the T-1 signal sent by the Wave system. Do not modify this field unless specifically advised to do so by a Vertical Communications Customer Service representative.

The following table describes the configurable DSX parameters.

DSX configurable parameters

Display Name	Display Value	Allowed Values	Default Value
Cable Length	0 133 266 299 512 655 3000 6000	0 133 266 299 512 655 3000 6000	655
Receive Equalizer	On Off		On
Receive Input Threshold	1.36 V 1.04 V 0.84 V 0.62 V 0.43 V 0.32 V 0.22 V	1.36 V 1.04 V 0.84 V 0.62 V 0.43 V 0.32 V 0.22 V	1.36
Transmit Pulse Mask (do not modify)	Hex	0x0 to 0xFFFFFF	0x5a9301

Trunk timing values

You can find the Trunk Timers in the Trunk Configuration applet.

T-1 trunk timing values

The following table describes the different types of inbound T-1 Trunk timers for the E&M Wink Start and E&M Immediate Start signaling types.

Inbound T-1 trunk timers (E&M Wink Start and E&M Immediate Start)

Display Name	Description	Default Value (msec)
Hit Counter Limit	Not an actual timer, but a counter used to determine a rare condition where a test signaling pattern is being sent by the service provider. If the counter is exceeded, the channel enters an error state.	10
Answer Delay	Minimum delay before answer	70
Inter-Digit	Maximum wait for next digit	15000
Wink Duration (applicable to E&M Wink Start only)	Duration of transmit wink	190
Far-End Disconnect	Time to wait to determine that far-end has disconnected	300
Call Validate	Time to wait to determine that far-end has disconnected; delay before transmit wink	90
Near-End Disconnect	Time to wait after near-end hangs up for far-end to hang up before treating the situation as an error	300

The following table describes the different types of outbound T-1 trunk timers for E&M Wink Start and E&M Immediate Start signaling types.

Outbound T-1 trunk timers (E&M Wink Start and E&M Immediate Start)

Display Name	Description	Default Value (msec)
Error Duration	Length of time-out after an error before the channel is put back in service	30000
Far-End Disconnect	Time to wait to determine that far end has disconnected	250
Near-End Disconnect	Time to wait after near-end hangs up for far-end to hang up before treating the situation as an error	700
Wait Answer	Maximum wait for answer	0 (infinite)
Validate Answer	Minimum length of incoming off-hook to detect answer	600
Maximum Wink	Maximum duration of incoming wink allowed. Timeout is interpreted as GLARE	280
Validate Start Signal (applicable to E&M Wink Start only)	Minimum duration of wink	70)
Wait Start Signal (applicable to E&M Wink Start only)	Maximum wait for wink after near-end disconnects	5000
Wait Dial	Delay before dial after end of wink	100 (E&M Wink Start) 200 (E&M Immediate Start)
DTMF Duration (applicable to E&M Wink Start only)	Duration of DTMF tone on and off	100

The following table describes the different types of inbound trunk timers for signaling type ground start.

Inbound T-1 trunk timers (ground start)

Display Name	Description	Default Value (msec)
Hit Counter Limit	Not an actual timer, but a counter used to determine a rare condition where a test signaling pattern is being sent by the service provider. If the counter is exceeded, the channel enters an error state.	5
Inter-Digit	Maximum wait for next digit	10000
Call Validate	Time to wait to determine that far-end has disconnected; delay before disconnecting	90

The following table describes the different types of outbound trunk timers for signaling type ground start.

Outbound T-1 trunk timers (ground start)

Display Name	Description	Default Value (msec)
Error Duration	Length of time-out after an error before the channel is put back in service	30000
Validate Start Signal	Time to wait for dial tone before declaring a glare situation	4000
Wait Start Signal	Maximum wait for tip ground before declaring a glare situation	500
Far-End Disconnect	Minimum length of incoming on-hook when far-end disconnects first	250
Wait Dial	Delay before dial after tip ground and dial tone detected	10
DTMF Duration	Duration of DTMF tone on and off	100

The following table describes the outbound trunk timers for ISDN PRI.

Inbound T-1 trunk timers (ISDN PRI)

Display Name	Description	Default Value (msec)
Alert/Connect Timeout	Milliseconds after an offhook before an incoming call is processed	0
Inter-Digit	Maximum wait for next digit	8000
Maximum wait for Caller ID	Milliseconds after the first ring to wait for Caller ID	2000

Analog trunk timing values

The following table describes the different types of inbound analog trunk timers for loop start and ground start signaling types.

Inbound analog trunk timers (loop start and ground start)

Display Name	Description	Default Value (msec)
Ring detect trigger	Milliseconds of ringing to be detected by the microcontroller before being reported to the system software	250
CO drop (in/out)	Milliseconds of missing loop current detected by the microcontroller before a line drop event is reported to the system software	400
Disconnect	Maximum wait for far-end disconnect after near-end disconnect of incoming call before treating the situation as an error	10000
Subsequent Ring	Maximum time between subsequent rings before deciding that far-end has given up calling	8000
Offhook Delay	The delay between sending offhook and the switch connection being made. If callers hear noise when being connected to a call on this trunk, adjust this timer for an offhook delay of 160ms. Some experimentation will reveal the best setting. Loop start only.	10
Inter-Digit	Maximum wait for the next digit before routing the call	15000
Hold off, flash (in/out)	Milliseconds after a flash before line events are actively detected	500
Call Validate	Maximum time between first and second ring	7000
Hold off, onhook (in/out)	Milliseconds after an onhook before line events are actively detected	1500
Hold off, offhook (in/out)	Milliseconds after an offhook before line events are actively detected	800

The following table describes the different types of outbound analog trunk timers for loop start and ground start signaling types.

Outbound analog trunk timers (loop start and ground start)

Display Name	Description	Default Value (msec)
Error Duration	Length of time-out after an error before the trunk is put back into service	30000
Flash Duration	Length of hook flash sent to the far end.	500
Wait Start Signal	Maximum wait for tip ground before declaring a glare situation	5000
Disconnect	Maximum wait for far-end disconnect after near end disconnects an outbound call before treating the situation as an error	2000
Wait Dial	Delay before dial after tip ground and dial tone detected	500
DTMF Duration	Duration of DTMF tone on and off	100

Chapter 35

Starting the TFTP Server

CHAPTER CONTENTS

Wave includes a Trivial File Transfer Protocol (TFTP) server component to support configuration of Vertical SIP phones.

Starting the TFTP Server

The TFTP Server is not started by default. The TFTP server is automatically started after you enter the first Wave IP User license in the Software Licenses applet. If you need to manually start the TFTP server for some reason, start it using the following procedure.

To start the TFTP server on your Wave system

1 Click the Vertical Wave Desktop icon in the Management Console.

Click

2 Click **OK** to clear the warning message that is displayed.

Note: When you launch certain Microsoft Windows tools from the Global Administrator Management Console, they start up in a remote control window that allows tools or applications running on the server (the Wave system in this case) to appear on the client (your workstation). Each time you use one of these tools, you will perform a remote control log on. See “Remote access applets” on page 2-7 for detailed information and an example.

3 Log on to Windows. Enter your user name and password. The initial default logon values are:

> **User Name**. `GlobalAdministrator`
>
> **Password**. `Vertical4VoIP!`

Note: Password is case-sensitive.

4 Click **Start > All Programs > ModMgr**. The Vertical Communications Component Manager (ModMgr) dialog opens.

5 Scroll down the list to locate the service called “VNI TFTP Service”.

6 Click on **Start** to start the service. The service will be started and will only run until stopped or until the Wave is restarted. It will not be restarted after a reboot.

7 Close all open windows on the desktop.

8 Choose **Start** and then **Log Off** to return to the Management Console.

Part 5

Appendices

Appendix A

Protecting Your Phone System Against Toll Fraud

CHAPTER CONTENTS

Businesses using any phone system, including Wave ISM, are vulnerable to loss of money from unauthorized people hacking into their phone system. Hackers can then make hundreds of outbound long distance or international calls that cost businesses around the world millions of dollars every year. Wave contains several features and options that can protect your system against toll fraud.

Typical toll fraud strategies

While hackers committing toll fraud use a variety of techniques to gain access to a system, it is important to note that 99% of the time access is gained through unsecure, easy-to-guess passwords. Wave ISM System Settings provide several options to enforce harder-to-guess passwords.

The following are the most common methods of attempted toll fraud:

- Calling the main auto attendant, pressing #, logging in as the Administrator, pressing # for dial tone and placing outbound calls.
- Attempting to log on at every extension (101, 102, etc.) until an extension with an easy password is found. Once found, the hacker will change call forwarding to the external number they want to dial (for example, an international number or the number of another hacked PBX), and then make calls to the external number as needed. By calling through multiple hacked PBXs, Caller ID and traces will be unable to track down the hacker's identity.
- Calling random users and telling them they are a representative from the phone company and need their voice mailbox password to track down a problem with the phone system. Users should be told to never give out their passwords, and if they have reason to believe someone else has it, to change it immediately to something secure.

Identifying toll fraud

The following methods will help you tell whether your system has been targeted by toll fraud hackers:

- Check the Call Log in the User/Group Management applet daily for multiple logon attempts. A failed logon attempt will show as “logon - Abandoned”. A successful fraudulent logon will typically show many long distance or international calls placed afterwards from that extension.

  Note: You can have Wave automatically hang up on callers and lock out accounts after multiple failed logon attempts. See “Enforcing strong password security” on page 4-14.

- Check your phone bills carefully for international numbers or long distance numbers you do not recognize.
- Watch your Trunk Monitor (available on the Diagnostics tab of the Management Console) for sudden bursts where every line is busy with people trying to log on.

Securing your system against toll fraud

The following are a variety of ways to secure your phone system. While practicing all of these strategies will keep your phone system very secure, by far the most important strategy is to just improve the security of passwords.

Password security

Wave System Settings gives you several options for making user passwords more secure. For maximum security you should choose all of the following options:

- Set a minimum password length. Passwords should be at least 5 digits long, preferably 7 or more.
- Prevent passwords from including the user’s extension.
- Prevent passwords from including easy-to-guess elements like same-digit strings (111) or consecutive-digit strings (123).
- Regularly force password change.

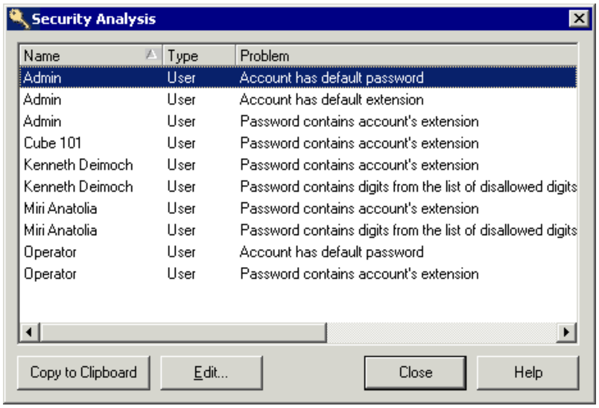
For more information about password security via the System Settings dialog, see “Enforcing strong password security” on page 4-14

Changing the Admin and Operator passwords

Wave’s two default users, the Admin and Operator, have easy-to-guess passwords. Immediately after installing Wave, you should change the passwords on those accounts to something more secure, by editing those users in the Users view. Reminder messages in the User/Group management applet will warn you if you leave the extensions as is.

Identifying users with security-risk passwords

The User/Group Management applet has a built-in Security Analysis report that analyzes passwords used on your system for potential security risks. To run the Security Analysis report, choose **Tools > Analyze Security**. The Security Analysis report opens on-screen.



Name	Type	Problem
Admin	User	Account has default password
Admin	User	Account has default extension
Admin	User	Password contains account's extension
Cube 101	User	Password contains account's extension
Kenneth Deimoch	User	Password contains account's extension
Kenneth Deimoch	User	Password contains digits from the list of disallowed digits
Miri Anatolia	User	Password contains account's extension
Miri Anatolia	User	Password contains digits from the list of disallowed digits
Operator	User	Account has default password
Operator	User	Password contains account's extension

Use the report to determine which users in your system have passwords that make your system vulnerable. If you have implemented the security options described in this section, few users should appear in the list. Those who do might have old passwords that have not yet been changed, either because they have not yet logged in and been forced to change their passwords, or because they are exempt from forced password change. Talk to those users about making their passwords more secure.

You can address your security problems directly from the dialog by selecting an item and clicking **Edit** to open the User dialog for the user.

Disallowing security-risk user permissions

Disallow security-risk permissions for all users except those individuals who really need them. You can change permissions for individual users by editing the user account. You can also use security roles to restrict permissions globally and easily assign a group of permissions just to users who need them. See “Managing roles” on page 11-122 for details.

Security-risk permissions which should be disallowed are:

- Place external calls when logged on via a trunk (under the Standard permission group)
- Log on via trunk (Standard)
- Log on via IP trunk (Standard)
- Log on via station (Standard)
- Forward or route calls to external numbers (Standard)
- Return calls when logged on via a trunk (Standard)
- Select a specific trunk for outbound call (Administration)

Setting up dialing restrictions

A good way to prevent unauthorized outbound calling is to place restrictions on users' dialing permissions. You can change dialing permissions using access profiles in Outbound Routing and then assign that access profile at the user- or user-template level.

Some dialing restrictions to consider:

- Disallow access to any number dialed during toll fraud. To find a list of numbers, search your call logs for frequent calls to international locations.
- Disallow dialing 011 and 00 to block all international calls (00 dials the international operator).

  To permit some international calls you can do the following:

  - Enable 011 for those individuals who are authorized to make international calls. Those individuals can then dial any country.
  - Enable country codes for those foreign countries that are appropriate for users to call. To do so, enable 011xxx where xxx is the desired country code.

The full list of country codes can be found in your phone book. The list is maintained by the ITU (International Telecommunication Union), a division of the United Nations. The ITU web site is **http://www.itu.int** and the most recently published list of country codes is available at **http://www.itu.int/itudoc/itu-t/ob-lists/icc/e212_685.html** (this list is valid as of January 2004, and some additional country codes have been assigned since then.)

- Disallow dialing sequences that call for-pay services like 1900 or 1976, 976, etc. For information on additional numbers that should be blocked, see this website:

  http://www.lincmad.com/telesleaze.html

- Disallow dialing certain international North American area codes if desired, such as those in the Caribbean. For example, disallowing 1242 blocks calls to the Bahamas.

  The full list of North American area codes can be found in your phone book or at the web site for the North American Numbering Plan Administration:

  http://www.nanpa.com

Making account logon more secure

There are several ways to prevent hackers from even getting to the account logon menu pick of your auto attendant. Some methods make it difficult for your own users to use the system, so you need to judge how far you want to go to prevent toll fraud at the expense of phone system ease of use. Note that these options do not make your system secure by themselves, as they only slow down hackers. The only way to make account logon secure is to make sure your user passwords are secure and are changed often.

Auto attendant security options include the following:

- **In your main auto attendant, change the default logon menu pick "#" to another value.** Be sure to tell users what key to press to log on.
- **Only allow logon from certain auto attendants**. Give your remote users a phone number routed to a special auto attendant that permits remote logon, and prevent your main auto attendant from doing so. For DID systems (where you can't control the specific trunk used on inbound calls), give your remote users a DID number instead that routes them to the special auto attendant.

- **Rotate the auto attendant that supports logon**. Do not permit logon in your main auto attendant that is assigned to every trunk. Instead, each week create a unique auto attendant that permits logon on a different trunk. Publish the trunk's phone number to your users as it changes.
- **Enable auto logon for users and auto attendants**. When auto logon is set up for a user, whenever the user calls into Wave from the specified phone number via an auto logon-enabled auto attendant, the user is automatically logged in to his or her voice mailbox without being prompted to enter an extension or password. You configure this option for each user via the "The User \ Numbers tab" on page 11-26.

Securing your phone system database

Toll fraud typically involves "hacking" over phone lines instead of data hacking. However, the Wave database runs on a Windows server on your network and contains all permission settings and can be hacked at that level. It is always wise to keep your corporate network secure from unauthorized external access. This safeguards your database against tampering by network and computer hackers. Some ways to do this include:

Use standard firewall technology to secure access to your network. If desired, allow access to specific protocols and ports, such as those for HTTP (VoIP).

Securing SIP stations

If your system uses SIP phones as external stations, hackers can gain entry to the system by sending a SIP message that duplicates the SIP URI of a SIP phone user, for example, vwilliams@sip:www.Vertical.com. Without protection, Wave assumes the call is coming from the external station and automatically logs it in and provides internal dial tone, permitting the caller to place outbound calls through Wave.

To protect against SIP fraud, you can do the following:

- Make sure that each SIP phone uses authentication credentials whenever it connects to Wave.
- If your system interacts with an external SIP server, such as a PSTN gateway or a SIP provider (IPSP), set up two SIP spans, one to handle SIP stations and the other to handle traffic from the external SIP server.

Checking for current scams

Most phone carriers maintain toll fraud web pages with current information. You can monitor these web sites for up-to-date information and potential remedies. Contact your carrier for more information.

Responding to toll fraud attempts

If your phone system has been the target of toll fraud attempts, you can do the following:

- Report Caller ID numbers and called numbers of fraudulent calls to your long distance carrier. Sometimes carriers can block certain numbers from calling you.
- Report excessive toll fraud to your local FBI office. Note, however, that the FBI does not usually get involved with toll fraud unless losses are substantial.

You can also use the information from previous toll fraud attempts to make your system even more secure. For example, you can add any numbers being called during toll fraud to the list of numbers prevented with dialing permissions. If fraudulent calls have been made to a particular few countries that are not otherwise called, disallow dialing those country codes (011xxx).

Third-party Software License Agreements

APPENDIX CONTENTS

XML parsing software

Wave includes derived XML parsing software copyrighted by the Apache Software Foundation.

The Apache Software License, Version 1.1

Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Xerces" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation and was originally based on software copyright (c) 1999, International Business Machines, Inc., http://www.ibm.com. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

PuTTY executables and source code

Refer to http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified and complies with the Debian Free Software Guidelines.)

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

WinSCP

WinSCP is open source software released under the GNU General Public License. (See “GNU General Public License” on page B-7.) Source code for WinSCP can be downloaded from:

http://winscp.net/download/winscp382source.zip

Wireshark

Wireshark is open source software released under the GNU General Public License. (See “GNU General Public License” on page B-7.)

http://www.wireshark.org/

TFTP Server

Wave includes derived TFTP software copyrighted by the GNU General Public License (see page B-1), the University of California, the University of Washington, and the Leland Stanford Junior University. The source for the GPL portions of the software is available by contacting the office of the President or the office of the CTO at Vertical Communications, Inc.

The following statements refer to those portions of the software copyrighted by The Regents of the University of California:

Copyright (c) 1983, 1993 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following statements refer to those portions of the software copyrighted by the University of Washington and the Leland Stanford Junior University:

Copyright 1997 by the University of Washington/Stanford

Original version Copyright 1988 by The Leland Stanford Junior University

Copyright 1997 by the University of Washington

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both the above copyright notices and this permission notice appear in supporting documentation, and that the name of the University of Washington or The Leland Stanford Junior University not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. This software is made available “as is”, and

THE UNIVERSITY OF WASHINGTON AND THE LELAND STANFORD JUNIOR UNIVERSITY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, WITH REGARD TO THIS SOFTWARE, INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND IN NO EVENT SHALL THE UNIVERSITY OF WASHINGTON OR THE LELAND STANFORD JUNIOR UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR STRICT LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Openfire

Openfire is an instant messaging (IM) and groupchat server that uses the XMPP protocol. The Openfire source code is governed by the GNU Public License (GPL), which can be found in the LICENSE.html file in Openfire’s distribution. Openfire also contains Open Source software from third-parties. Licensing terms for those components is specifically noted in the relevant source files.

Openfire contains icons and images licensed from INCORS GmbH. All other images are owned by Jive Software. All icons and images in Openfire are provided under the following license agreement:

License Agreement

This is a legal agreement between You, the User of the Openfire application (“The Software”), and Jive Software (“Jive Software”). By downloading the Software, you agree to be bound by the terms of this agreement.

All ownership and copyright of the images and icons included in the Software distribution remain the property of Jive Software and INCORS GmbH. Jive Software grants to you a nonexclusive, non-sublicensable right to use the icons royalty-free as part of Openfire.

You may not lease, license or sub-license the icons, or a subset of the icons, or any modified icons to any third party. You may not incorporate them into your own software or design products.

All icon files are provided “As is” without warranties of merchantability and fitness for a particular purpose. You agree to hold Jive Software harmless for any result that may occur during the course of using the licensed icons.

This License Agreement shall be governed and construed in accordance with the laws of Oregon. If any provision of this License Agreement is held to be unenforceable, this License Agreement will remain in effect with the provision omitted.

Copyright © Jive Software, 2007

GNU General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

Acronis Standard EULA

ACRONIS
End User License Agreement (EULA)

BEFORE USING THE ACRONIS SOFTWARE ("SOFTWARE") OR ACRONIS ONLINE BACKUP SERVICE ("SERVICE"), YOU SHOULD CAREFULLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT") THAT APPLIES TO THE SERVICE. THIS AGREEMENT GOVERNS YOUR USE OF ANY SOFTWARE, INCLUDING ANY UPDATES THAT MAY BE PROVIDED TO YOU AND ANY ACCOMPANYING WRITTEN DOCUMENTATION AND THE ("SERVICE"). BY REGISTERING FOR THIS SERVICE YOU FULLY ACCEPT AND AGREE TO ALL OF THE PROVISIONS OF THIS AGREEMENT. OTHERWISE, PLEASE DO NOT REGISTER FOR THIS SERVICE. REGISTERING FOR THE SERVICE OR OTHERWISE USING THE SERVICE ESTABLISHES A BINDING AGREEMENT BETWEEN YOU AS THE PERSON USING THE SERVICE ("LICENSEE") AND ACRONIS INTERNATIONAL GMBH LOCATED AT: VERWALTUNG EURO HAUS RHEINWEG 9, SCHAFFHAUSEN, CH-8200, SWITZERLAND, ("LICENSOR"). IF YOU DO NOT ACCEPT ALL OF THE TERMS OF THIS AGREEMENT, YOU SHALL HAVE NO RIGHT TO DOWNLOAD OR USE THE SOFTWARE OR SERVICE.

You acknowledge and agree that Acronis may occasionally send you administrative communications regarding your account or the Software and/or Service via email. Please see the Acronis Privacy Policy, which is incorporated into this Agreement by reference.

TERMS AND CONDITIONS

ACCOUNTS, PASSWORDS, AND SECURITY

The Software and Service are intended and offered only for lawful use by individuals or organizations with the legal capacity and authority under applicable law to enter into a contract for such products or services. Acronis does not offer the Software or Service to minors or where prohibited by law. By registering for and/or by using the Software and/or Service, you represent and warrant that you have the legal capacity and authority to enter into a binding agreement to adhere to this Agreement, and that you will use the Software or Service only in accordance with these Terms and Conditions and with all applicable laws. If an individual is registering or using the Software or Service on behalf of an entity or organization, that individual warrants, represents, and covenants to Acronis that such individual is duly authorized to agree to these Terms and Conditions on behalf of the organization and to bind the organization to them. You agree to provide accurate and complete information when you register for the Service and you agree to keep such information accurate and complete during the entire time that you use the Service. You must be a registered user to access the Service. You are solely responsible for any consequences arising in whole or in part out of your failure to maintain the confidentiality of your username and/or password. You will be solely responsible and liable for any activity that occurs under your user name. You may access the Software or Service only through the interfaces and protocols provided or authorized by Acronis. You agree that you will not access the Software or Service through unauthorized means, such as unlicensed software clients. Certain Software or Service backup only certain types of files. You agree not to circumvent these limitations in any way, including but not limited to, changing file extensions or header information.

If you lose your password or the encryption key for your account, you may not be able to access your data. You are solely responsible for protecting the information on your computer such as by installing anti-virus software, updating your applications, password protecting your files, and not permitting third party access to your computer. You understand that the Software or Services may back-up files that are no longer usable due to corruption from viruses, software malfunctions or other causes. This might result in you restoring files that are no longer usable.

CUSTOMER EXPERIENCE PROGRAM

Acronis has instituted an Acronis Customer Experience Program (CEP), the details of which can be found at http://www.acronis.com/company/cep-policy.html, which also contains information regarding your ability to opt in/opt out of the CEP.

ACCEPTABLE USE AND CONDUCT

You are solely responsible for your conduct and your data related to the Service. The Software and Service are made available to you only for your personal use, which use must be in compliance with all applicable laws, rules and regulations and must not infringe or violate third party rights. You may not make commercial use of the Software or Service, including but not limited to selling or distributing the Software and/or Service to any third party. Any unauthorized use of any Acronis computer system is a violation of this Agreement and certain federal and state laws. Such violations may subject the unauthorized user and his or her agents to civil and criminal penalties.

You may not use the Software or Service for any unlawful purpose. Without limiting generality of the foregoing:

(a) The Software or Service may not be used to store, backup, or distribute child pornography and may not be used in violation of U.S. export control laws or the export or import regulations of other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain licenses to export, re-export, or import as may be required.

(b) You may not use the Software or Service if you are a citizen, national, or resident of, or are under control of, the government of Cuba, Iran, Sudan, Libya, North Korea, Syria, or any other country to which the United States has prohibited export. Each time you use the Software or Service you represent, warrant, and covenant that: (i) you are not a citizen, national, or resident of, nor under the control of, any such country to which the United States has prohibited export; (ii) you will not download or otherwise export or re-export the Software, directly or indirectly, to the above mentioned countries nor to citizens, nationals or residents of those countries; (iii) you are not listed on the U.S. Department of Treasury's Lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, the U.S. Department of State's List of Statutorily Debarred Parties, or the U.S. Department of Commerce's Denied Persons List, Entity List, or Unverified List Table of Denial Orders; (iv) you will not download or otherwise export or re-export the Software, directly or indirectly, to persons on the above mentioned lists; (v) you will neither use nor allow the Software to be used for, any purposes prohibited by United States federal or state law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical, or biological weapons of mass destruction; (vi) the Software will not be exported, directly, or indirectly, in violation of these laws, nor will the Software or Services be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation; and (vii) you are not using or permitting others to use the Software or Service to create, store, backup, distribute, or provide access to child pornography.

Acronis may block your access to your backup data and/or terminate your use of the Software or Service if Acronis reasonably believes that the backup data may contain child pornography or are being used to support other types of illegal activities, if providing the Software or Service to a person located in a particular country would violate U.S. or other applicable law, or if your continued use of the Software or Service may damage, disable, overburden, or impair our servers or networks.

Acronis will not decrypt your files unless i) it reasonably believes that it must do so to troubleshoot problems with the Service or ii) it reasonably believes it must do so in order to comply with any law, subpoena, warrant, order, or regulation. Acronis may also provide access to your data to government authorities if Acronis suspects or believes that the data contain child pornography or other prohibited data or that the data are being used for illegal purposes. You acknowledge that Acronis or Acronis affiliates may use servers and other equipment to provide the Software or Service that are located in the United States or in other countries where litigants, law enforcement, courts, and other agencies of the government may have the right to access data stored within their jurisdictions upon terms and conditions provided by local law, and that as a result, they may gain access to your backup data as provided by applicable local law.

You agree to indemnify, defend, and hold harmless Acronis, its officers, directors, employees and its suppliers from any and all loss, cost, liability, and expense arising from or related to your data, your use of the Service, or your violation of these terms. You agree to reimburse Acronis for any costs or fees related to its enforcement of this Agreement, including without limitation the expert fees and attorney fees regularly charged by the experts and legal counsel chosen by Acronis.

FAIR USE POLICY

ACRONIS SHALL HAVE THE ABSOLUTE AND UNILATERAL RIGHT IN ITS SOLE DISCRETION TO DENY USE OF AND ACCESS TO ALL OR ANY PORTION OF THE SOFTWARE OR SERVICE TO USERS WHO ARE DEEMED BY ACRONIS TO BE USING THE SOFTWARE OR SERVICE IN A MANNER NOT REASONABLY INTENDED BY ACRONIS OR IN VIOLATION OF LAW, INCLUDING BUT NOT LIMITED TO SUSPENDING OR TERMINATING A USER'S ACCOUNT WITH ACROIS AND THE LICENSE TO USE THE SOFTWARE OR SERVICE.

The Software or Service is designed to serve the needs of particular types of users, i.e. individual consumers or business accounts. If you have purchased a Service that is inappropriate for your actual usage, Acronis may require you to switch to an appropriate Service. Acronis may, in our sole discretion and from time to time, establish or amend general operating practices to maximize the operation and availability of the Software or Service and to prevent abuses. As part of these practices, we reserve the right to monitor our system to identify excessive consumption of network resources and to take such technical and other remedies as we deem appropriate. Your consumption of the Service may be deemed excessive if, within any month, your usage greatly exceeds the average level of monthly usage of Acronis' customers, generally. In the event you are deemed to have violated this policy, we reserve the right to offer an alternative pricing plan or Service that will permit you to continue to use the Service. We also reserve the right to terminate or suspend your license to use the Software or Service, without prior notice, in the event of a violation of this policy.

CONSENT TO COLLECT NON-PERSONAL INFORMATION; USE OF DATA; ENCRYPTION

The Software and Service may collect certain non-personally identifiable information that resides on your computer, including, without limitation, statistics relating to how often backups are started and completed, performance metrics relating to the Software, and configuration settings. This information collected will be sent to Acronis and may be used by Acronis without restriction. When you back up data via the Service, you agree that we and our service providers may copy and store such data as part of the Service. The Software or Service may permit you to decrypt and download backup data from any Internet enabled computer. You understand that by electing to access your files from a computer other than the one you used to create the backup data, that your backup data will be decrypted by Acronis in its data center and sent to you in a decrypted format via public infrastructure. You acknowledge that this may cause the contents of these files to become accessible to individuals other than you and that you accept this risk. You further acknowledge that depending upon the Software or Service you use or the features of the Software or Service you use that accessing your backup data from any Internet enabled computer many not be possible.

CHANGES TO THE SERVICE AND TERMS AND CONDITIONS

Acronis reserves the right at any time to modify, suspend, or discontinue providing the Service or any part thereof in its sole discretion with or without notice. However, Acronis will use commercially reasonable efforts to notify you of modification, suspension, or discontinuance of the Service either by sending an email to the email address you provide with your registration or by a posting on the acronis.com website. However, in no event will Acronis be liable to you or to any third party for any modification, suspension or discontinuance of the Service with or without notice.

From time to time, Acronis may issue new releases, revisions, or enhancements to the Software or Service available to you free of charge or for a fee. New releases, revisions or enhancements may be licensed, downloaded, and installed only to the extent that you hold a valid license to use the Software or Service being updated or upgraded, and you may use them only in accordance with Acronis' then-current Terms and Conditions of Use and any additional license terms that may accompany them.

Acronis reserves the right at any time to modify this Agreement in its sole discretion, without liability to you. This Agreement, as amended, will be effective upon acceptance of registration for new users and effective for all existing users 15 days after the posting of any amended terms on the acronis.com website. You agree to be bound by this Agreement, as modified. If you do not agree to any changes to this Agreement, you must terminate your account immediately, which shall be your sole and exclusive remedy.

USE OF SOFTWARE

1. Offline Software. Subject to the terms and conditions of this Agreement, upon purchase of a license to Acronis' "offline" Software (i.e. not hosted by Acronis), Acronis grants and you accept a non-exclusive, nontransferable, non-assignable license to use Software in accordance with its documentation, only for your own internal use solely on the specific number of computers that you have licensed. Installation of the Software is your responsibility. If Acronis identifies the Software as an evaluation version, trial version or beta version, you have the right to use the Software for such limited purpose for the period found at http://www.acronis.com/homecomputing/download/ (the "Trial Period') unless extended by Acronis in writing. Software licensed under such a limited license may not be used in a production environment. At the conclusion of the Trial Period, unless a standard license to the Software is purchased by you, you will delete the Software from your computer(s) and have no further license or other rights with respect to the Software except as to the rights and responsibilities in this Agreement. By virtue of licensing Software and registering your Software with Acronis, and at Acronis' sole discretion, you are entitled to: (1) "patch" or "dot releases (e.g., 11.01, 11.02, and 11.03 etc.) of the Software. A major release(s) of the Software (e.g., Version 12 Version 13, etc) are not included in support and would require a paid upgrade fee; (2) support consistent with Acronis' current support policies as found in the support section of the Acronis web site (specified in the product and/or documentation) or any relevant contract between you and Acronis. ;and (3) other electronic services that Acronis may make generally available to its customers, such as an electronically available base of knowledge ("Knowledge Base") to assist in answering general questions about the Software. In the event that you makes any unauthorized modifications to the Software, Acronis' obligations to provide support services are null and void. Support policies are subject to change, but generally will include basic support for thirty (30) days following purchase. Proof of payment and/or registration is required to obtain support.

2. Online Software. Subject to the terms and conditions of this Agreement, Acronis grants you a non-exclusive, non-transferable, non-sublicensable license to, for your internal use only, install and execute one (1) copy of the Software (in executable code form only) only on a single computer and only for the purpose of accessing and using the Service.

3. General Terms Applicable to Software and Service. The Software and its structure, organization, source code, and documentation contain valuable trade secrets of Acronis and its licensors, and accordingly you agree not to (and agree not to allow third parties to) (1) sublicense, lease, rent, loan, transfer, or distribute the Software and/or Service or any derivative thereof to any third party, (2) modify, adapt, translate, or prepare derivative works from the Software or Service, (3) decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Software or Service, (4) decrypt data or extract portions of the Software's files for use in other applications, (5) remove, obscure, or alter Acronis' or any third party's trademarks or copyright or other proprietary rights notices affixed to or contained within or accessed in conjunction with or through the Software or Service, (6) use or permit the Software or Service to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Acronis, or (7) publicly disseminate performance information or analysis (including, without limitation, benchmarks) from any source relating to the Software or Service. In addition, certain third party code may be provided with the Software and/or Service. The third-party license terms accompanying such code, which may be found at http://kb.acronis.com/content/7696 and in the license.txt file located in the root installation directory, and not the terms of this Section, will govern your use of such code.

You may use a license for the Software or Service, with only one computer at a time unless the Software or Services you use are explicitly designed and marketed to operate on more than one computer at a time concurrently. The type of license you have (including such variables as whether the license permits use of Software or Service on more than one computer, whether the licenses fees are based on the number of computers, volume of data, or both, and the length of the license periods, etc.) is set forth as part of the Software or Service description available at www.acronis.com. Should your license for the Software or Service you use be designed for only one computer at a time you may transfer your license to another computer in the event that you cease to use the computer on which the Software was originally installed. If you wish to protect multiple computers, you must obtain a separate paid license for each computer or you must obtain a multi-computer license which will be applicable to the number of computers stated in such license.

You agree that if i) you mark a file to no longer be backed-up, ii) you delete a file from your computer, iii) move a file to a location on your computer that is not marked for back-up, iv) you delete a computer from your Software or Service account, v) your computer is unable to access the Service, or vi) you terminate or allow your trial or license to terminate, non-renew, or otherwise lapse for any reason, that the files you have marked, deleted, moved or stored on a deleted, inaccessible, or unlicensed computer may not be available to you should you wish to restore them.

INTELLECTUAL PROPERTY

You acknowledge that Acronis or third parties own all right, title and interest in and to the Software and Service, portions thereof, or software or content provided through or in conjunction with the Software or Service, including without limitation all intellectual property rights. Except for the license granted in this Section, all rights in and to the Software and Service are reserved, and no implied licenses are granted by Acronis.

If you have comments on the Software or Service or ideas on how to improve them, please email us at qaonl@acronis.com. Please note that by doing so, you also grant Acronis a perpetual, royalty-free, irrevocable, transferable license, with right of sublicense, to use and incorporate your ideas or comments into the Software or Service (or third party software, content, or services), and to otherwise exploit your ideas and comments, in each case without further compensation.

SUPPORT

Acronis is under no obligation to provide technical support under the terms of this license, and provides no assurance that any specific errors or discrepancies in the Software will be corrected.

TERM AND TERMINATION

This Agreement is effective upon your download of and access to the Software and Service and remains in effect until your account is terminated. You may terminate this Agreement at any time by destroying the Software and closing your account by following the instructions on the acronis.com website.

This Agreement automatically terminates if you fail to comply with its terms and conditions. Acronis reserves the right to refuse or discontinue participation to any user at any time at its sole discretion. You agree that, upon such termination, you will destroy and permanently erase all copies of the Software and that your access rights to the Service will immediately terminate. The terms of the Sections entitled Consent to Collect Non-Personal Information, Intellectual Property, Disclaimer of Warranties, Limitation of Liability, and Miscellaneous will survive expiration or termination.

If this Agreement terminates, other than for your failure to comply, Acronis will use commercially reasonable efforts to make your data available for you to download for a period of three (3) days. Acronis has no obligation to provide you with a copy of your data and may remove and discard any data. You also agree that Acronis may retain your personal information and related account information for a reasonable time after your license has been terminated.

FEEDBACK FROM LICENSEE

It is expressly understood, acknowledged and agreed that Licensee shall, regardless of whether or not formally requested to do, provide to Acronis reasonable suggestions, comments and feedback regarding the Software, including but not limited to usability, bug reports and test results, with respect to Software testing (collectively, "Feedback"). Contingent upon all of the terms and conditions herein and especially upon Licensee's obligations to provide Feedback, Licensee grants Acronis, under all of Licensee's intellectual property and proprietary rights, the following worldwide, non-exclusive, perpetual, irrevocable, royalty free, fully paid up rights: (i) to make, use, copy, modify, sell, distribute, sub-license, and create derivative works of, the Feedback as part of any Acronis product, technology, service, specification or other documentation (individually and collectively, "Acronis Products"); (ii) to publicly perform or display, import, broadcast, transmit, distribute, license, offer to sell, and sell, rent, lease or lend copies of the Feedback (and derivative works thereof) as part of any Acronis Product; (iii) solely with respect to Licensee's copyright and trade secret rights, to sublicense to third parties the foregoing rights, including the right to sublicense to further third parties; and (iv) to sublicense to third parties any claims of any patents owned or licensable by Licensee that are necessarily infringed by a third party product, technology or service that uses, interfaces, interoperates or communicates with the feedback or portion thereof incorporated into a Acronis Product, technology or service. Further, Licensee warrants that Licensee's Feedback is not subject to any license terms that would purport to require Acronis to comply with any additional obligations with respect to any Acronis Products that incorporate any Feedback.

DISCLAIMER OF WARRANTIES

THE SOFTWARE AND SERVICE AND ANY THIRD PARTY SOFTWARE AND SERVICES ARE PROVIDED "AS IS," WITH NO WARRANTIES WHATSOEVER. ACRONIS AND SUCH THIRD PARTIES EXPRESSLY DISCLAIM TO THE FULLEST EXTENT PERMITTED BY LAW ALL EXPRESS, IMPLIED, AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT OF PROPRIETARY RIGHTS AND ANY WARRANTIES REGARDING THE SECURITY, RELIABILITY, TIMELINESS, AND PERFORMANCE OF THE SOFTWARE OR SERVICE AND SUCH THIRD PARTY SOFTWARE OR SERVICES. ACRONIS DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE

SOFTWARE OR SERVICE WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE OR SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE OR SERVICE WILL BE CORRECTED. ACRONIS DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR SERVICE IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY OR OTHERWISE. ACRONIS DOES NOT REPRESENT OR WARRANT THAT USERS WILL BE ABLE TO ACCESS OR USE THE SOFTWARE OR SERVICES AT TIMES OR LOCATIONS OF THEIR CHOOSING, OR THAT ACRONIS WILL HAVE ADEQUATE CAPACITY FOR ANY USER'S REQUIREMENTS. NO ORAL OR WRITTEN STATEMENT, INFORMATION OR ADVICE GIVEN BY ACRONIS, OR ITS RESPECTIVE EMPLOYEES, DISTRIBUTORS, DEALERS, OR AGENTS SHALL CREATE ANY WARRANTIES.

YOU UNDERSTAND AND AGREE THAT YOUR DOWNLOAD AND/OR USE OF THE SOFTWARE AND SERVICE, AND ALL THIRD PARTY SOFTWARE OR SERVICES MADE AVAILABLE IN CONJUNCTION WITH OR THROUGH THE SOFTWARE OR SERVICE, IS AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGES TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF THE SOFTWARE OR SERVICE AND SUCH THIRD PARTY SOFTWARE AND SERVICES.

SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE AND JURISDICTION TO JURISDICTION.

LIMITATION OF LIABILITY

UNDER NO CIRCUMSTANCES SHALL ACRONIS, OR ITS SUPPLIERS, RESELLERS, PARTNERS OR THEIR RESPECTIVE AFFILIATES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES ARISING FROM OR RELATED TO THE SOFTWARE OR SERVICE, WHETHER SUCH CLAIM IS BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, (EVEN IF ANY SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES). WITHOUT LIMITING THE FOREGOING, THE TOTAL AGGREGATE LIABILITY OF ACRONIS, AND ITS SUPPLIERS, RESELLERS, PARTNERS AND THEIR RESPECTIVE AFFILIATES ARISING FROM OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT, IF ANY, PAID BY YOU TO ACRONIS FOR THE SOFTWARE OR SERVICE. IF THE SOFTWARE AND SERVICE ARE

PROVIDED WITHOUT CHARGE, THEN ACRONIS AND ITS SUPPLIERS SHALL HAVE NO LIABILITY TO YOU WHATSOEVER.

THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY WHETHER THE DAMAGES ARISE FROM USE OR MISUSE OF AND RELIANCE ON THE SOFTWARE OR SERVICE, FROM INABILITY TO USE THE SOFTWARE OR SERVICE, TO USE OR RETRIEVE ANY BACKUP DATA, OR FROM THE INTERRUPTION, SUSPENSION, OR TERMINATION OF THE SOFTWARE OR SERVICE (INCLUDING SUCH DAMAGES INCURRED BY THIRD PARTIES). SUCH LIMITATION SHALL APPLY NOTWITHSTANDING A FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND TO THE FULLEST EXTENT PERMITTED BY LAW. SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR INCIDENTAL, CONSEQUENTIAL, OR DIRECT DAMAGES, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

THE SOFTWARE AND SERVICE ARE NOT INTENDED FOR USE IN CONNECTION WITH ANY NUCLEAR, AVIATION, MASS TRANSIT, OR MEDICAL APPLICATION OR ANY OTHER INHERENTLY DANGEROUS APPLICATION THAT COULD RESULT IN DEATH, PERSONAL INJURY, CATASTROPHIC DAMAGE, OR MASS DESTRUCTION, AND LICENSEE AGREES THAT LICENSOR WILL HAVE NO LIABILITY OF ANY NATURE AS A RESULT OF ANY SUCH USE OF THE SOFTWARE.

GOVERNMENT END USERS

This Agreement applies to all Software and Service acquired directly or indirectly by or on behalf of the United States Government. The Software and Service are commercial products, provided on the open market at market prices, and was developed entirely at private expense and without the use of any U.S. Government funds. If the Software or Service is supplied to the Department of Defense, the U.S. Government acquires only the license rights customarily provided to the public and specified in this Agreement. If the Software or Service is supplied to any unit or agency of the U.S. Government other than the Department of Defense, the license to the U.S. Government is granted only with restricted rights. Use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c) of the Commercial Computer Software Restricted Rights clause of FAR 52.227-19.

MISCELLANEOUS PROVISIONS

You acknowledge and agree that the Software which is the subject of this Agreement may be controlled for export purposes. You agree to comply with all United States export laws and regulations, and you shall not and shall not allow any third-party to remove or export from the United States or allow the export or re-export of any part of the Software or Service or any direct product thereof: (i) into (or to a national or resident of) any embargoed or terrorist-supporting country; (ii) to anyone on the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals; or (iii) to any country to which such export or re-export is restricted or prohibited, or as to which the United States government or any agency thereof requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval. You warrant that you are not located in, under the control of, or a national or resident of any such prohibited country or on any such prohibited party list. The Software and Service is further restricted from being used for the design or development of nuclear, chemical, or biological weapons or missile technology, or for terrorist activity, without the prior permission of the United States government. You assume sole responsibility for any required export approval and/or licenses and all related costs and for the violation of any United States export law or regulation. This Agreement shall be governed by the laws of the Commonwealth of Massachusetts, exclusive of its conflicts of laws provisions and without regard to the United Nations Convention on Contracts for the International Sale of Goods, and any suit under this Agreement shall exclusively be brought in a federal or state court in Massachusetts. Any action against Acronis under this Agreement must be commenced within one year after such cause of action accrues.

The failure of Acronis to exercise or enforce any right or provision of this Agreement does not constitute a waiver of such right or provision. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, the remainder of this Agreement will continue in full force and effect. This Agreement, which incorporates the Acronis Privacy Policy, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. Any waiver of any provision of this Agreement will be effective only if in writing and signed by Acronis.

You may not assign or transfer any of your rights or obligations under this Agreement to a third party without the prior written consent of Acronis. Acronis may freely assign this Agreement. Any attempted assignment or transfer in violation of the foregoing will be void from the beginning.

CONTACTING ACRONIS

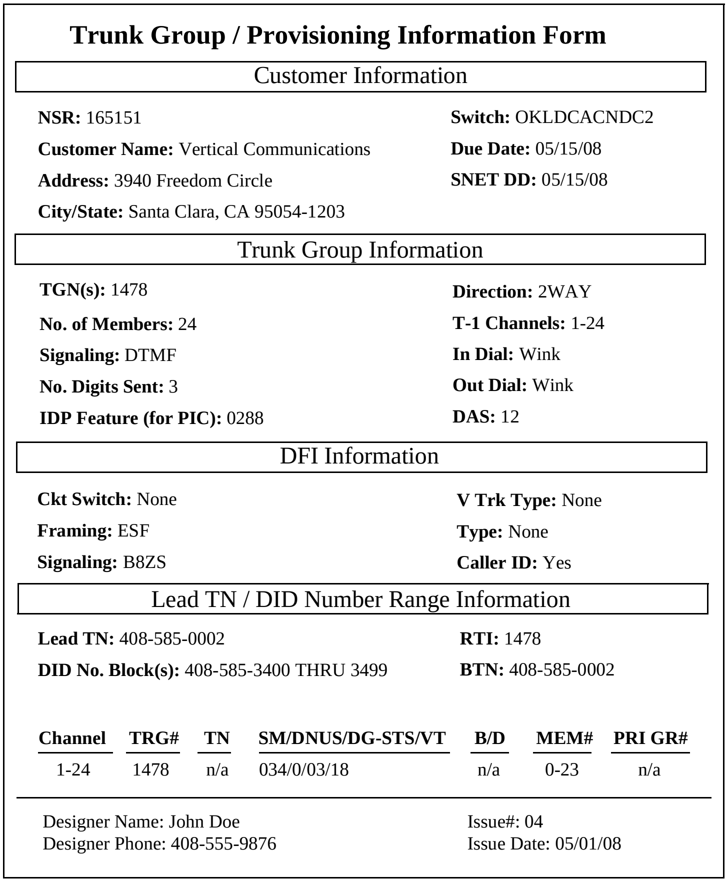
Users with questions about this Agreement or the Privacy Policy may contact Acronis at: www.acronis.com/support.

Service Confirmation Letters and Provisioning Information Forms

CHAPTER CONTENTS

The sample provisioning information form and service confirmation letter shown in this appendix are included to help you better understand the type of information you need to obtain from your service provider so that you can configure your T-1 or analog trunks. Note that these sample forms may be different from those used by your service provider.

Sample trunk provisioning information form



Trunk Group / Provisioning Information Form

Customer Information

NSR: 165151	**Switch:** OKLDCACNDC2
Customer Name: Vertical Communications	**Due Date:** 05/15/08
Address: 3940 Freedom Circle	**SNET DD:** 05/15/08
City/State: Santa Clara, CA 95054-1203	

Trunk Group Information

TGN(s): 1478	**Direction:** 2WAY
No. of Members: 24	**T-1 Channels:** 1-24
Signaling: DTMF	**In Dial:** Wink
No. Digits Sent: 3	**Out Dial:** Wink
IDP Feature (for PIC): 0288	**DAS:** 12

DFI Information

Ckt Switch: None	**V Trk Type:** None
Framing: ESF	**Type:** None
Signaling: B8ZS	**Caller ID:** Yes

Lead TN / DID Number Range Information

Lead TN: 408-585-0002	**RTI:** 1478
DID No. Block(s): 408-585-3400 THRU 3499	**BTN:** 408-585-0002

Channel	TRG#	TN	SM/DNUS/DG-STS/VT	B/D	MEM#	PRI GR#
1-24	1478	n/a	034/0/03/18	n/a	0-23	n/a

Designer Name: John Doe
Designer Phone: 408-555-9876

Issue#: 04
Issue Date: 05/01/08

Sample trunk service confirmation letter

Your trunk confirmation letter from your service provider will contain information similar to that in the sample letter that follows.

> Dear Administrator:
>
> The information that follows confirms the services to be provided by the XYZ Telecommunications Group to Vertical Communications at 3940 Freedom Circle, Santa Clara, CA 95054:
>
> (24) 2-way Digital Trunks
>
> Block of DIDs
> 408-585-3200 through 3299
>
> T-1 Framing B8ZS-ESF
>
> Wink Start Signaling
>
> 3-digit delivery
>
> RJ-48X Jack Termination
>
> The above service is targeted to be delivered by November 23, 2006. I will provide you with periodic updates as I receive them. Please contact me should you have any questions.
>
> Sincerely,
>
> Sue Simpson
> Regional Account Service Coordinator

Wave Port Usage

CHAPTER CONTENTS

This appendix describes Wave Server port usage and configuration requirements.

Wave Global Administrator port usage

This section describes ports used by the Global Administrator Management Console.

Port Type	Receive On	Transmit On	Configurable	Notes
Standard Global Administrator access	TCP 80	TCP 80	No	Used to access the Global Administrator Management Console.
Wave License Activation Server	HTTPS Secure SSL 443	HTTPS Secure SSL 443	No	Used for “one-click” Wave license activation requests via the Vertical License Activation Server (https://activate.vertical.com). See “One-click vs. offline activation” on page 24-12.
Wave License Proxy Server	TCP 11003	TCP 11003	No	Used to process “offline” Wave license activation requests via an optional proxy server on another PC on your network that acts as an interface between your Wave Server and the Vertical License Activation Server. See “Setting up a proxy server for license activation” on page 24-20 for more information.

IP telephony port usage

This section describes ports used with IP telephony. For details on how to set up IP telephony on a Wave Server, see Chapter 6.

Wave SIP port usage

This section describes SIP ports usage.

Port Type	Receive On	Transmit On	Configurable	Notes
RTP	UDP/dynamic (16384-18384)	UDP/ Dependent on other endpoint	No	
RTCP	UDP/dynamic (16385-18385)	UDP/ Dependent on other endpoint	No	
SIP Station Transport	Default = 5060.	Dependent on other endpoint	Yes. Any valid port in IP Telephony Listener Port.	The default port, 5060, is generally used for IP telephony, but if this port is already in use in your system, you can specify another port. Specified when you configure a SIP Signaling Control Point (SCP). See “Configuring Signaling Control Points” on page 6-14.
SIP Trunk Transport	Default = 5060.	Dependent on other endpoint	Yes. Any valid port in IP Telephony Listener Port.	The default port, 5060, is generally used for IP telephony, but if this port is already in use in your system, you can specify another port. Specified when you configure a SIP Signaling Control Point (SCP). See “Configuring Signaling Control Points” on page 6-14.
Music on Hold	UDP (65000-65010)	UDP/ Dependent on other endpoint		

When using Voice Over IP in a network, especially one that includes a firewall, you will need to know the ports used in the packets that carry VoIP traffic. The following table lists the ports used in the packets.

	Receive on...	Transmit to...
RTP Voice Transport		
RTP	UDP/dynamic (16384 - 18384) - not configurable	UDP/Dependant on other endpoint
RTCP	UDP/dynamic (16385 - 16835) - not configurable	UDP/Dependant on other endpoint
SIP Transport		
	5060 - configurable to 5061	5060, 5061
	UDP 65000 (used for music on hold)	

Aastra SIP port usage

This section describes SIP ports usage with Aastra SIP phones.

Port Type	Receive On	Transmit On	Configurable	Notes
SIP	5060	5060		Default port for SIP signaling.
RTP	UDP (3000)	UDP (3000)		Default port for RTP audio.
RTCP	UDP (3001)	UDP (3001)		Default port for RTCP.
TFTP	UDP (69)	UDP (69)		Port for requesting and downloading configuration file from the Wave Server.

WaveNet port usage

This section describes the port used by Microsoft Message Queue (MSMQ) to communicate between WaveNet nodes. For more about planning for, configuring, and using WaveNet, see Chapter Chapter 25.

Port Type	Receive On	Transmit On	Configurable	Notes
TCP	TCP 1801	TCP 80		Used if you select the **TCP** Communication Method when you add a Wave Server to a WaveNet network. **Note:**

Note: In addition to the port described above, SIP ports are also required to support call routing and other communications between WaveNet nodes. See “Wave SIP port usage” on page D-2.

Wave Add-on port usage

This section describes port usage and configuration requirements for Wave Add-ons available at the time this manual was last updated. For information about other Wave Add-ons, see the documentation included with the Add-on.

Wave Global Manager port usage

Source	Source Port	Destination	Destination Port	Application	Notes
Global Manager Server	TCP 1004	Wave Server	TCP 10004	Global Manager	Communication between Global Manager and Global Reporter Agent.
Global Manager Server	Any/Dynamic	FTP Server	TCP 21	FTP	Upload and download HotFixes and Reports.
Global Manager Console	Any/Dynamic	Global Manager Server	TCP 1433	Global Manager Console	ODBC client communication between Global Manager Console and SQL Server.
Global Manager Console	Any/Dynamic	FTP Server	TCP 21	FTP	Upload HotFixes.

For more about installing, configuring, and using Wave Global Manager, see the *Wave Global Manager Administrator Guide*.

Wave Global Reporter port usage

Source	Source Port	Destination	Destination Port	Application	Notes
Global Reporter Server	TCP 1024-5000	Global Manager Server	TCP 134	MSTDC	Communication between Global Manager Server and Global Manager Agent. **Note:** This port is not opened if Global Manager and Global Reporter are installed on the same system.
PC accessing Global Reporter reports	Any/Dynamic	Global Reporter Server	TCP 80	Global Reporter Server	Access Global Reporter web server via HTTP.
Global Reporter Server	Any/Dynamic	FTP Server	TCP 21	FTP	Download data files.
Global Reporter Server	Any/Dynamic	Global Reporter Server	TCP 1433	SQL Server	Access SQL Server from Global Reporter Server. **Note:** This port is not opened if SQL Server and Global Reporter are installed on the same system.

For more about installing, configuring, and using Wave Global Manager, see the *Wave Global Reporter Administrator Guide*.

Index