Vocera Voice Server Administration Console Guide

Version 5.2.3

Notice

Contents

VOCERA VOICE SERVER ADMINISTRATION CONSOLE GUIDE

Getting Started

This section provides an overview of the Vocera Voice solution, and describes how to use the Vocera Control Panel, the Administration Console, and the documentation.

About the Vocera Administration Guide

The Vocera Voice Server Administration Console Guide describes how to perform tasks using the Administration Console.

You can use this reference as you work with the Administration Console, and you can get the same information from the console's context-sensitive help. The organization of this guide generally matches the layout of the Administration Console.

For information about configuration telephony integration and using pagers and other wireless devices with Vocera, see the separate Vocera Voice Server Telephony Configuration Guide, the Vocera Voice Server Administration Console Guide describes how to perform tasks using the Administration Console.

About the Vocera System Software

This section describes the Vocera system software.

Main Components

Learn about the main components of Vocera Voice Server system software.

The Vocera system software includes the following main components:

- **Vocera Voice Server Program**—provides the central system functionality, and calls on the other components for specific services.
- **Embedded MySQL Database™** —stores user profiles (which contain personal information and badge settings), group and location information, and system settings.
- **Nuance™ Recognition Server and Vocalizer™ Software** —provides the speech recognition and text-to-speech engines used by the Vocera voice interface.
- **Apache / Tomcat Web Server**—hosts the browser-based Administration Console and User Console applications.

Software Utilities for Badge Configuration

Review a brief description for the Badge Properties Editor and Badge Configuration Utility.

The Vocera system software includes the following utilities:

- **Badge Properties Editor**—lets you set values for badge properties so the Vocera badges can connect to the wireless network. See the *Vocera Device Configuration Guide*.
- **Badge Configuration Utility**—downloads the properties you set with the Badge Properties Editor, as well as any firmware upgrades, to your badges. See the *Vocera Device Configuration Guide*.

Specialized Modules

Learn about the modules provided for working with Vocera Voice Server system software.

The Vocera Voice Server system software includes the following specialized modules:

- The **Vocera System Tray Icon** appears in the server notification area at the right of the taskbar on the Vocera Voice Server, Vocera SIP Telephony Gateway, and Vocera Client Gateway. The Vocera system tray icon changes to indicate the current running state of the Vocera system. The system tray provides access to the Vocera Control Panel, which lets you control the server.
- The **Vocera launcher** is a Windows service that starts automatically when the computer boots. The launcher starts the Vocera Voice Server and the associated services it requires, such as the MySQL, Nuance, and Apache/Tomcat components, as well as the optional Vocera Telephony Solution Software, if installed.

- **Administration Console**, a browser-based application, provides the interface to the Vocera Voice Server. See the *Vocera Voice Server Administration Console Guide* or the Administration Console's online help for an overview.
- **User Console**, also a browser-based application, allows individual users to set their own badge preferences and maintain their own contact information. See the *Vocera Voice Server Administration Console Guide* for information about logging in and granting access. See the *Vocera Voice Server User Console Guide* for detailed information.

Optional Software Components

Learn about the other products that you can implement with Vocera Voice Server.

Vocera also offers the following optional software components:

- **Vocera SIP Telephony Gateway** integrates the Vocera Voice Server with your telephone system, allowing badges and telephones to communicate seamlessly. The telephony software provides a Session Initiation Protocol (SIP) telephony gateway between the Vocera Voice Server and an IP PBX or a Voice over Internet Protocol (VoIP) gateway. Vocera SIP Telephony Gateway supports non-SIP enabled PBXs via Dialogic Media Gateway or other SIP/TDM gateway products.
- **Vocera Client Gateway** supports client devices and smartphones and Vocera Collaboration Suite clients, providing a signaling and multimedia gateway from the phones to the Vocera Voice Server for all calls.
- **Report Server Software** uses log files generated by the Vocera Voice Server to create an extensive set of reports. Some reports can help you spot usage trends, keep track of badges, and monitor call volume. Other reports help you diagnose end-user and network issues related to the Vocera system.
- **Vocera Messaging Interface**Vocera Messaging Interface enables two-way messaging between the Vocera Communications System and third-party applications, such as nurse call systems, patient monitoring systems, supply management systems, point of sale and other store management applications, network management software, HVAC, industrial alarms and other enterprise applications. The Vocera Messaging Interface supersedes the nurse call interface offered with earlier versions of Vocera.
- **Vocera Administration Interface** is a Java API that enables you to control and administer the Vocera system programmatically.

Vocera Technical Support Tools and Software Utilities

Learn how to work with Vocera Technical Support tools and utilities.

When you install the Vocera Voice Server, the installation program also installs tools and utilities that can be used to facilitate the exchange of Vocera Voice Server information with Vocera Technical Support and to aid in troubleshooting. These tools provide the best way to send server logs and other debugging data and tasks you can use when working with Vocera Technical Support.

The utilities below are launched from the Windows Start menu:

- **Change Server IP Address**—The Vocera SIP Telephony Gateway, and Vocera Client Gateway need to know the IP address(es) of the Vocera Voice Server. You enter this IP address(es) when you install the software but you can also launch the utility and change the IP address as needed.

- **Enable Dual Recognition Server** —Allows you to enable and disable Dual Speech Recognition in order to improve speech recognition. You can enable a second recognition server when you install the software. In addition and after installation, you can launch the utility and change the setting as desired.

- **Update SSL and Connector Settings** —Enabling SSL on the Vocera Voice Server affects how Vocera Messaging Platform and clients connect to the server. You can enable SSL when you install the software. In addition and after installation, you can launch the utility and change the setting as desired.

For more information about more available support tools, see the `readme.txt` file located in the `\vocera\support` folder on your Vocera Voice Server, and contact Vocera Technical Support.

Using the Vocera Control Panel

Learn how to use the Vocera system tray icon to display the Vocera Control Panel, which lets you control the Vocera Voice Server.

Vocera System Tray Icon

Learn about the use and function of the Vocera system tray.

When the Vocera Voice Server, Vocera SIP Telephony Gateway, or Vocera Client Gateway server starts running, the Vocera system tray icon appears in the server notification area at the right of the taskbar.

Figure 1: System tray

You can use the Vocera system tray icon to start the Vocera Control Panel for your user session. The Vocera Control Panel displays status messages and lets you control the server.

Note: Windows 2008 R2 systems may require additional configuration to add the Vocera Control Panel system tray options to the notification area.

The Vocera system tray icon changes to display the status of the server:

Table 1: Vocera system tray icons

Icon	Description
	The server is running. You can use the Vocera system tray icon to start the Vocera Control Panel.
	The server is not running. You can use the Vocera system tray icon to start the server.
	The server is processing a stop or start request.

To display the Vocera Control Panel:

•
  Right-click the Vocera system tray icon , and select the following command appropriate for your server:
  • Vocera Voice Server = **Vocera Control Panel**
  • Vocera SIP Telephony Gateway = VSTG Control Panel
  • Vocera Client Gateway = VCG Control Panel
  The Control Panel window appears on the desktop.

Note: On the Vocera Voice Server, a Command Prompt window called Vocera Launcher Console also appears. It displays status messages as Vocera processes are started and stopped.

To start up the server:

*   Right-click the Vocera system tray icon , and select the following command appropriate for your server:
    *   Vocera Voice Server = Start Vocera
    *   Vocera SIP Telephony Gateway = Start VSTG
    *   Vocera Client Gateway = Start VCG

    The Control Panel window appears on the desktop.

Displaying Vocera Control Panel Help

Learn how to display Vocera Control Panel help when using the Vocera User Interface.

The Vocera Control Panel has online help that displays in your browser.

To display Vocera Control Panel help:

*   Choose Help > Contents.
    The help opens in your browser.

Vocera Control Panel Menus

Learn about the Vocera Control Panel commands and functionality.

Table 2: Control Panel menus

Menu	Command	Description	Servers
Run	Start	Starts the server.	VS, VSTG, VCG
	Stop	Temporarily suspends the server.	
	Shutdown	Shuts down the server.	
Display	Normal	Displays only the most significant system events. This is the default.	VS only
	Detailed	Displays all events.	
	Off	Displays no events.	
Cluster	Start Standalone	Temporarily removes a Vocera Voice Server from a cluster and restarts it as a standalone system.	VS only
	Failover	Fails over to the standby Vocera Voice Server, or restarts the server if it's currently in standby.	
Server	IP Address(es)	Specifies the Vocera Voice Server IP address(es) used by the server.	VSTG, VCG
Help	Contents	Displays online help.	VS, VSTG, VCG
	About	Displays version information.	

Determining the Status of the Server

The Vocera Control Panel provides a status indicator below the menu bar at the top of the screen.

The indicator displays one of the following states to tell you whether the server is available for use:

Table 3: Control Panel status

Status	Description
● Active	The server is running and available for use. A standalone Vocera Voice Server is always active unless you have stopped it. A Vocera Voice Server that is part of a cluster is active when it is the primary machine, unless you have stopped it.
● Standby	The server is running but is not available for use. A Vocera Voice Server that is part of a cluster is in the standby state when it is one of the secondary machines.

Stopping and Restarting the Server

Learn how to start and stop the sever, the conditions under which should, and the affect to the clients.

In certain situations, you may need to stop and restart the server. For example, if you want to update the properties in all your badges at the same time, you must stop the Vocera Voice Server and then restart it.

You may want to restart the server when only a few people are using the system. When the server is stopped, clients are unable to connect and communication is temporarily suspended:

- When the Vocera Voice Server is stopped, users cannot communicate with their badges.
- When the Vocera SIP Telephony Gateway is stopped, users cannot place or receive phone calls.
- When the Vocera Client Gateway is stopped, users cannot communicate with the Vocera Collaboration Suite app or with Vocera Smartphones.

The server stops and starts fairly quickly, so if few people are using the system, there will be very little interruption.

> **Note:** You can also use the Server page of the Maintenance screen in the Administration Console to stop and start the server.

To stop and restart the server:

1. In the Vocera Control Panel, choose Run > Stop, or click ◼.
   The Control Panel displays messages indicating that the server has stopped.

2. Choose Run > Start, or click ▶.
   The Control Panel displays messages indicating that the server has started.

Controlling the Display of Events

On the Vocera Voice Server, the Vocera Control Panel displays a continuously scrolling list of system events, letting you view the system status at a glance.

You determine the level of detail that the Control Panel displays through settings that you make in the menus. You can specify any of the following settings on the Display menu of the Vocera Control Panel:

- **Normal** displays only the most significant system events in the Control Panel. This is the default.
- **Detailed** displays all events in the Control Panel.
- **Off** displays no events in the Control Panel.

Vocera records all system events in the system log files, regardless of the setting you make for the display of events.

Using the Cluster Menu

Learn the commands that you can use to control your cluster and a description of each.

On a Vocera Voice Server that is part of a cluster, the Vocera Control Panel has a Cluster menu that lets you control the cluster. For example, you may want to force a failover when you add a new machine to a cluster, or you may want to start one of the machines as a standalone Vocera Voice Server.

The Cluster menu provides the following commands:

Table 4: Cluster menu commands

Command	Description
Start Standalone	Temporarily removes a Vocera Voice Server from a cluster and restarts it as a standalone system. This command *does not* break up a cluster or cause a failover to occur; instead, it allows you to disconnect a server from a cluster temporarily for maintenance. The exact behavior of this command depends upon the state of the server at the time that you stopped it: • If the Vocera Voice Server was *active* and badges were connected to it, the badges reconnect when you start the node as a standalone system. • If the Vocera Voice Server was in *standby* mode, it restarts as an active standalone server, and it does not interfere with the active node of the cluster in any way. The Start Standalone command is available only when the Vocera Voice Server is stopped. See **Stopping and Restarting the Server** on page 18 for more information about stopping the server. The Cluster Setup page on the System screen in the Administration Console does not get updated when you execute the Start Standalone command. That is, the Enable Cluster checkbox remains selected, all the servers remain in the list, and the status of the servers in the list does not change. When you restart a standalone server, it goes into discovery mode and comes online as a cluster node in the same state—active or standby—it was in prior to becoming a standalone server. You can restart a standalone server with either the Failover command in its Vocera Control Panel or the Force Restart button on the Cluster Setup page of its Administration Console.
Failover	Does one of the following, depending on the status of the Vocera Voice Server: • If the server was *active*, this command causes control of the cluster to fail over to one of the standby machines. • If the server was in *standby* mode, this command restarts the server, but does not cause control of the cluster to fail over. • If the server was running as a standalone server, this command restarts the server as a cluster node in the same state—active or standby—it was in prior to becoming a standalone server.

If failover occurs in a clustered environment, the control panel opens to the active server instance.

Changing the Vocera Voice Server IP Address

Follow these steps to change the Vocera Voice Server IP address.

The Vocera SIP Telephony Gateway, and Vocera Client Gateway need to know the IP address(es) of the Vocera Voice Server. You enter this IP address(es) when you install the software. However, you can use the Vocera Control panel to change the address.

To change the Vocera Voice Server IP address used by the server:

1. In the Vocera Control Panel, choose Server > IP Address(es).
   The IP Address dialog box appears.
2. Use the **Server IP Address** field to provide the address of the Vocera Voice Server.

Enter the numeric IP address using dot notation. For example:

192.168.15.10

For a Vocera Voice Server cluster, enter a comma-separated list of IP addresses. For example:

192.168.15.10,192.168.15.11,192.168.15.12

3. Click OK.

   The dialog box closes, and the server begins using the new Vocera Voice Server IP address immediately.

Shutting Down the Vocera Voice Server Server

Follow these steps to stop the Vocera Voice Server.

When you shut down the server, you stop the Vocera Voice Server and all its related services. In the case of the Vocera Voice Server, this includes MySQL, Tomcat, Apache Web Server, and Nuance.

To shut down the server:

1. In the Vocera Control Panel, choose Run > Shutdown.
   A confirmation dialog box appears.

2. Click **OK**.

   The dialog box closes, and the Control Panel also closes.

   If you shut down the Vocera Voice Server, the launcher Command Prompt window displays messages indicating that Vocera and its related services are stopping. When all Vocera services have stopped, the Command Prompt window closes.

Using the Administration Console

This section describes how to get started using the Administration Console.

The Vocera Administration Console is a browser-based application that allows you to configure the Vocera Voice Server and the Vocera SIP Telephony Gateway.

Browser Requirements

Learn the Internet Explorer requirements needed to access Vocera Web applications.

To access Vocera Voice Web applications (Administration Console, User Console, Report Console, and Staff Assignment), your computer must have the following required software:

Table 5: Web application software requirements

Applications	Client-side component	Requirement
All applications	Browser	Internet Explorer versions 10 or later (Be sure that Compatibility Mode is turned off).

Important: Do not install another JRE on the Vocera Voice Server or Vocera Report Server machines. The required version of Java is installed with those servers.

Browser Recommendations and Requirements

Learn other important recommendations and tasks to internet and browser security.

The list below includes the configuration recommendations for Internet Explorer security settings. Required items are flagged.

- **Do not access a Vocera Voice Web application from the server on which it is running** – By default, Windows Server 2008 and Windows Server 2012 ship with Internet Explorer Enhanced Security Configuration enabled, which may display frequent security prompts when you access a Web application from the server on which it is running. Rather than disable Internet Explorer Enhanced Security Configuration on the server, we recommend that you access Vocera Voice Server Web applications from your desktop or laptop computer.
- **Configure the Internet Explorer security level to Medium-low or lower** – Otherwise, Internet Explorer prevents the scripts used by the consoles from executing completely. You can configure security settings through Tools > Internet Options > Security in Internet Explorer. See your Internet Explorer documentation for complete information.
- **Required: Disable the pop-up blocker** – Vocera consoles display information in pop-up windows, so disable pop-up blocking in Internet Explorer (that is, configure the browser to allow pop-up windows). Choose Tools > Internet Options > Privacy, and then uncheck the Turn On Pop-Up Blocker box.

  If you are using a third-party tool to block pop-ups, refer to the tool's documentation.

- **Remove scroll bars from pop-up windows** – Pop-up windows may display scroll bars. To remove the scroll bars, choose Tools > Internet Options > Security, and select the Local Intranet zone. Click Custom Level to display the Security Settings dialog box. Enable Allow script-initiated windows without size or position constraints.

- **Required: If necessary, add the Vocera Voice Server and Vocera Report Server IP addresses to the list of Trusted Sites** – The security policy in certain situations may prevent you from setting the Internet Explorer security level for the local intranet below Medium. If Internet Explorer continues to display pop-up windows with scroll bars, follow these steps to configure a trusted site for the Vocera Voice Server:

  To add the Vocera Voice Server and Vocera Report Server to the list of trusted sites:

  1. In Internet Explorer, choose Tools > Internet Options. The Internet Options dialog box appears.
  2. Click the Security tab.
  3. Click Trusted Sites.
  4. In the Security Level for this Zone box, set the security level to Medium-low, and click Apply.
  5. Click the Sites button. The Trusted Sites dialog box appears.
  6. Type the IP address of the Vocera Voice Server, and click Add.
  7. Type the IP address of the Vocera Report Server, and click Add.
  8. Click Close to close the Trusted Sites dialog box.
  9. Click OK to close the Internet Options dialog box.

  A system administrator can manage the Internet Explorer Trusted Sites for an entire organization using Group Policy Objects (GPOs).

- **If your Vocera Voice Server or Vocera Report Server has enabled SSL, configure Internet Explorer to NOT save encrypted pages to disk** – If you enable SSL on the Vocera Voice Server or Vocera Report Server, you may need to update the browser security settings for Internet Explorer to make sure the browser does delete cached-from-HTTPS resources when the browser is closed. Otherwise, certain pages of the Administration Console, such as the Permission Browser, will not work properly.

  To update Internet Explorer security settings for SSL access:

  1. In Internet Explorer, choose Tools > Internet Options > Advanced.
  2. Make sure the Do not save encrypted pages to disk option is checked.
  3. Click OK.

Logging In

Learn about accessing the Administration Console.

The Administration Console lets you manage a Vocera system. It is a browser-based application, accessible from any computer on the network.

The console URL is either of the following, where *vocera_ip_address* is the numeric IP address of the Vocera Voice Server:

Table 6: Administration Console URLs

Type of Access	URL
Unencrypted	`http://` *vocera_ip_address* `/console/adminindex.jsp`
SSL	`https://` *vocera_ip_address* `/console/adminindex.jsp`

After you complete the initial setup and your organization starts using Vocera, access the Administration Console from a computer that is not running the Vocera Voice Server so you don't degrade system performance.

Logging In Using Active Directory Authentication

When Active Directory authentication is enabled, the Administration Console welcome page has an additional field, the Active Directory list, which specifies the Active Directory to use for your login.

To log into the Administration Console using Active Directory credentials:

1. Open an Internet Explorer browser window.
2. Enter the Administration Console URL to open the Administration Console welcome page.
3. Specify the following values:

Field	Description
User ID	Enter your Active Directory user ID (up to 250 characters). You must be a member of a Vocera group that has administrator privileges.
Password	Enter your Active Directory password (up to 127 characters).
Active Directory	Select the name of your Active Directory from the list. If there are multiple Active Directories listed and you're unsure which one to select, ask your system administrator.

4. Click Log In.

    The Administration Console opens.
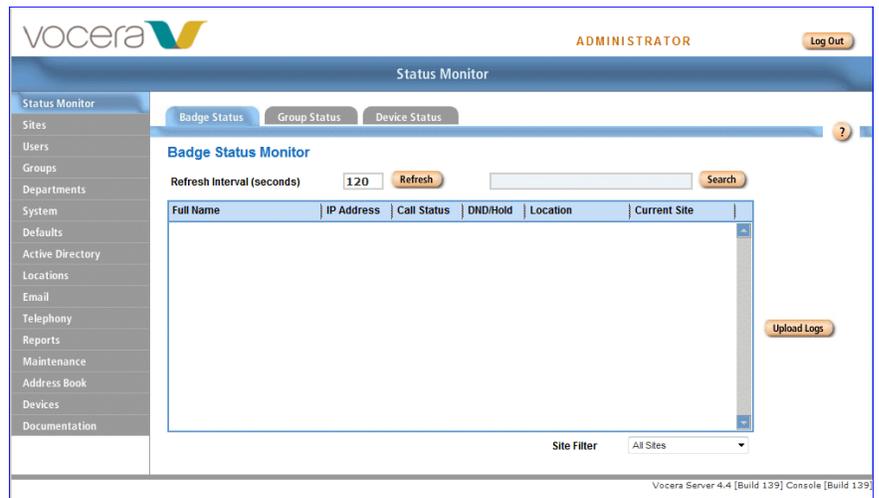
Figure 2: Administration Console opening screen

Logging In Using Vocera Authentication

If Active Directory authentication is not enabled, the Active Directory list does not appear on the Administration Console welcome page and you must log into the Administration Console using your Vocera credentials.

To log into the Administration Console using Vocera credentials:

1. Open an Internet Explorer browser window.
2. Enter the Administration Console URL to open the Administration Console welcome page.
3. Specify the following values:

Field	Description
User ID	Enter your Vocera user ID. You must be a member of a Vocera group that has administrator privileges.
Password	Enter your Vocera password.

4. Click Log In.

    The Administration Console opens.

Logging In Using the Default Administrator Account

Vocera provides a built-in administrator account with the user ID Administrator.

The default Administrator password is admin, but you can change it to something more secure.

Note: Regardless if Active Directory authentication is enabled, the default Administrator account does not use Active Directory credentials to log in.

Administration Console User Interface

Learn the basic User Interface controls on the Administration Console.

The following figure uses the Sites screen to show some of the user interface controls available in a typical Administration Console screen.
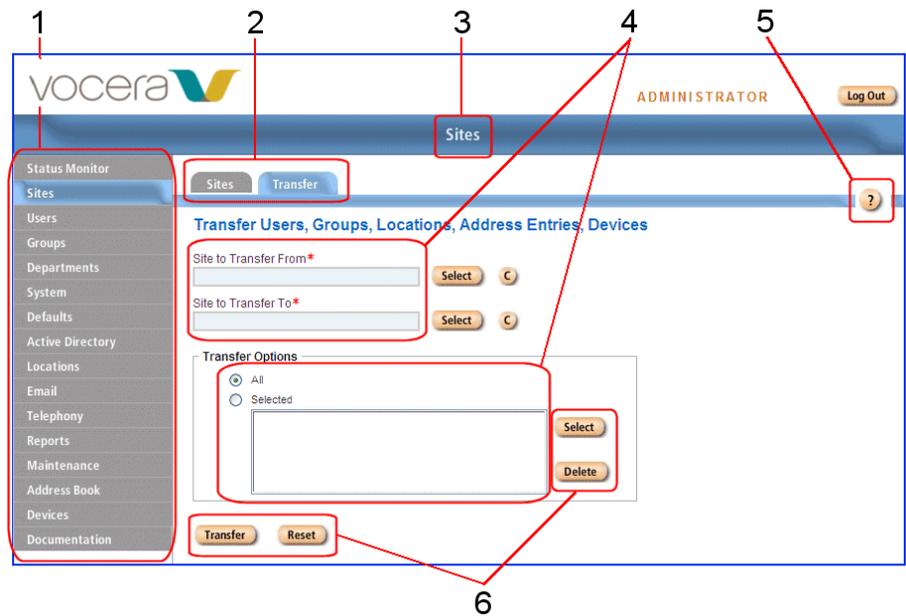
Figure 3: Administration Console user interface

1. **Navigation bar.** Click a button to display a screen.
2. **Tabs.** Click a tab to display a page in a screen.
3. **Screen title.** Displays the screen name.
4. **Fields.** Click a field to select or edit a value in a page.
5. **Help button.** Click the ? button to display context-sensitive help.
6. **Buttons**. Click a button in a page to perform an action.

Some pages have buttons that open dialog boxes. For example, when you click the Add New User button on the Users page, it opens the Add New User dialog box:

Figure 4: Add New User dialog box

Dialog boxes have tabs that group complex information to make it easier to enter and understand. Most have both a Save and Save & Continue button.

- Clicking Save will save the data and close the dialog.
- Clicking Save & Continue will save the data and clear the fields, leaving the dialog open to allow faster entry of new information.
- If you click Cancel, or close the dialog without clicking Save or Save & Continue, changes are discarded.

System and Tiered Administrators

Learn about administrator privileges available for Vocera Administration Console.

An *administrator* is a person who maintains the data in the Administration Console. Vocera lets you set up administrators with varying degrees of privileges:

- *System administrators* are individuals who have complete access to the Administration Console and full permissions for adding, editing, and deleting data in it. System administrators are often IT or telephony personnel who are not badge users.
  See System Administrators on page 25.
- *Tiered administrators* are individuals who have limited access to the Administration Console and restricted permissions for adding, editing, and deleting data in it. Tiered administrators are often badge users who have less of a technical background than system administrators.
  See Tiered Administrators on page 26.

System Administrators

System administrators have full permissions for adding, editing, and deleting data in the Administration Console.

When you log in to the Administration Console as a system administrator, you are:

- Given full administrative privileges in the Administration Console
- Automatically granted every other Vocera permission

As described in Setting Passwords on page 108, Vocera provides a default login to the Administration Console for initial access by system administrators. The user ID of the default login is `Administrator` and the initial password is `admin`. Logging in to the Administration Console with this default user ID provides full system administrator privileges.

Administrative Groups

Members of this *administration group* log into the Administration Console with their own user ID and password, but have full administrative privileges.

You should use the default `Administrator/admin` login only for initial access to the Administration Console. After initial access, you should create an administrative group, grant it the Perform System Administration permission, and populate it with members who will be system administrators.

The Perform System Administration permission includes all Vocera permissions except for three that administrators do not need. See System Administrator Permissions on page 234.

Vocera recommends using an administration group because the Vocera Report Server provides auditing capabilities that allow you to determine which user ID modified the database, and when the changes occurred. If multiple administrators use the default login, you cannot determine which individual made changes.

The Perform System Administration permission overrides any permissions revoked by membership in other groups, unless the Perform System Administration permission is revoked itself. For example, if a change to corporate policy prohibits toll calls, you can revoke Call Toll Numbers in the Everybody group. However, the Perform Server Administration permission overrides this setting,

Ongoing Maintenance

As use of the Vocera system grows, ongoing maintenance becomes increasingly important.

For example, you must add new users to the system and remove old members, set up alternate spoken names for users with nicknames, make changes to group membership over time, and so forth.

System administrators can optionally delegate some of the responsibility for ongoing maintenance to tiered administrators. See Tiered Administrators on page 26.

Tiered Administrators

Tiered administrators have permission to perform some of the maintenance duties typically handled by system administrators.

As with system administrators, tiered administrators acquire permissions to manage the database from membership in one or more groups.

Like all Vocera permissions, tiered administration permissions are *cumulative*—that is, you can assign multiple permissions to the same group and users can accumulate multiple permissions by membership in multiple groups. See Accumulating Permissions on page 83.

You can set up multiple groups of tiered administrators, creating tiers of access capabilities to further distribute maintenance. For example, you can assign one group the View Users and Groups permission, assign another group both the View Users and Groups and the Add/Edit/Delete Users permissions, and assign a third group all the tiered administration permissions.

Tiered administrators log in to the Administration Console with their own user IDs and passwords. Depending on their permissions, these administrators can see different sections of the Administration Console, and they may not be able to modify all that they can see. Tiered administrators must have a password to access the Administration Console.

The following table lists the Administration Console screens that are visible with each permission and summarizes the capabilities that each permission grants:

Table 7: Tiered administration permissions

Permission	Visible Sections	Capabilities
Add/Edit/Delete Users	Users	Add, edit, and delete users and all features of user profiles except group membership.
Edit Users	Users	Edit all features of existing user profiles except group membership.
Add/Edit/Delete Temporary Users	Users	Add, edit, and delete temporary users and all features of their profiles except group membership.
Add/Edit/Delete Address Book Entries	Address Book	Add, edit, and delete address book entries.
View Users and Groups	Status Monitor, Users, Groups, Reports, and Address Book	Monitor user and group activity, view their profiles, and generate lists of them in reports. Also view information about address book entries.
Perform System Device Management	Status Monitor, Devices	Add, edit, and delete device data, including device status values, for all sites. Also view the Badge Status Monitor and Device Status Monitor to display information about logged in users and devices that have been assigned to groups.

If a tiered administrator is also a member of a group with management capabilities, that administrator can view the Groups page through the Administration Console and perform both group management and tiered administrator tasks.

The combination of group management capabilities and tiered administrator permissions can be very effective, because group managers are able to perform a separate range of tasks that you often want tiered administrators to perform, such as adding and removing group members.

See Group Managers on page 67 for complete information about group management tasks.

Setting Up Tiered Administrators

Learn about the permissions for Tiered Administrators.

Like all permissions, tiered administration permissions can be associated with any group. However, Vocera recommends that you create dedicated groups just for tiered administration permissions, so you can clearly see which users have these permissions at a glance.

If you are going to implement tiered administration permissions, Vocera suggests that you set up one group for each permission, and then assign users to the groups necessary to grant them the proper set of permissions.

For example, you could create the following groups and assign each group its respective tiered administration permission:

* Tiered Admin-Add Edit Delete Users
* Tiered Admin-Edit Users
* Tiered Admin-Add Edit Delete Temporary Users
* Tiered Admin-Add Edit Delete Address Book Entries
* Tiered Admin-View Users and Groups
* Tiered Admin-Perform System Device Management

Groups such as the ones above sort together in the Administration Console and are clearly labeled, so they are easy to maintain.

Avoid assigning multiple tiered administration permissions to a single group such as View and Add Edit Delete Users, even if you only have one set of tiered administrators who all have the same permissions.

As your deployment grows, and your needs change, you may require tiered administrators with various sets of permissions, and several groups that each have multiple tiered administration permissions are difficult to maintain. Creating several groups, each with a single tiered administration permission as described above, is the best practice.

Administration Console Security

The Administration Console provides legitimate administrators convenient access to your Vocera data, allowing easy updates and maintenance.

The Administration Console also provides security features to help you control access and ensure the safety of your data.

SSL Access

SSL (Secure Sockets Layer) is a standard Internet protocol for securely exchanging information between two parties.

SSL encrypts transmitted data with two keys: a public key known to everyone, and a private key known only to the recipient.

By convention, an SSL connection uses a URL that begins with `https:`, instead of `http:`. For example, to open an SSL connection to the Administration Console you use a URL such as:
`https://` *vocera_ip_address* `/console/adminindex.jsp`

You can optionally enable SSL access in the Administration Console and the User Console of the Vocera Voice Server during installation. After installation, you can enable or disable SSL access as described in **Changing the SSL Configuration** on page 28.

Although enabling SSL encrypts the transmitted data, it does not provide other security. For instance, it does not provide client authentication.

If you enable SSL, you will experience a delay every time you save or transmit data. This performance delay is an unavoidable aspect of SSL encryption and can be mitigated somewhat by a fast CPU on the Vocera Voice Server and a high-bandwidth connection.

Note: If you want to enable SSL in a clustered environment, you must configure every server to use SSL. Do not configure some servers in a cluster with SSL and others without it.

Changing the SSL Configuration

After installation, you can enable or disable SSL by running the Update SSL and Connector Settings utility.

If you enable or disable SSL, you **do not** need to restart the server, as the server will automatically restart itself when you save changes in the Update SSL utility.

Enabling SSL on the Vocera Voice Server affects how Vocera Messaging Platform and clients connect to the server. If you enable SSL, there is additional configuration required to allow Vocera Messaging Platform and clients to connect to the Vocera Voice Server. For details, see Vocera Messaging Platform Administration Guide.

Important: If you are changing the SSL configuration on a Vocera Voice Server cluster, you should update the standby nodes before updating the active node. Update one standby node at a time. After you restart the server and the Vocera Control Panel finishes starting, wait until the status indicator displays the Standby status and a blue icon before updating the next standby node. When all the standby nodes have been updated, update

the SSL configuration on the active node of the cluster. When you restart the active node, it will automatically failover to a standby node, causing only a brief outage.

To enable or disable SSL:

1. Launch the Update SSL utility using either of two methods:

   1. Run *[vocera_drive]:\vocera\reports\tools\ConnectorConfig.exe*
   2. Use the **Update SSL and Connector settings** shortcut located from the Windows Start Menu.

   The **Update Tomcat Settings** dialog displays.

2. In the **Update Tomcat Setting** dialog, select the checkbox next to **Enable SSL** or uncheck the box to disable SSL.

3. Click **Apply Changes**.

   When you click **Apply Changes**, Apache 2.4 and Tomcat 8 services are stopped, the necessary registry entries and shortcuts are updated, and Apache 2.4 and Tomcat 8 services are restarted.

4. If you have a cluster installation, follow the previous steps to enable or disable SSL on every other machine in the cluster.

   Tip: Make sure you update the active node last.

5. If you change the SSL settings for Vocera Voice Server and also have Vocera Messaging Platform, make sure the VMP Server is properly configured to connect with the Vocera Voice Server. In the VMP Administrator, reconfigure options under System Options > Integrations > Vocera Voice, and then restart the server. See the *Vocera Messaging Platform Administration Guide* for details.

All changes made by the Update SSL utility is saved to a log file named **ConnectorConfig_5_2.log** in the *[SystemDrive]\nstallLogs-Vocera* directory.

Updating Browser Security Settings for SSL Access

If you enable SSL on the Vocera Voice Server, you may need to update the browser security settings for Internet Explorer to make sure the browser does not save encrypted pages to disk.

If you fail to do so certain pages of the Administration Console, such as the Permission Browser, will not work properly.

To update Internet Explorer security settings for SSL access:

1. In Internet Explorer, choose Tools > Internet Options, and then click the Advanced tab.
2. Make sure the Do not save encrypted pages to disk option is checked.
3. Click OK.

Creating a New SSL Certificate

Learn about setting up an SSL certificate.

When you configure SSL on the Apache web server during Vocera installation or afterward, an SSL certificate is created that is set to expire after 1825 days (5 years). The long duration of the certificate is intended for your convenience so that you do not need to replace it frequently on each Vocera Voice Server and on all Vocera smartphones. When the SSL certificate expires, you need to create a new one to enable access to the Administration Console and User Console and to allow Vocera smartphones to connect to the Vocera Voice Server. You can create the new SSL certificate while the Vocera Voice Server is running. However, you need to stop the Apache2 and Tomcat services temporarily.

If SSL is disabled or the certificate has not expired yet, you do not need to create a new certificate. If the URL you use to access the Administration Console starts with `https:` instead of `http:`, SSL is enabled. Another way to check whether SSL is enabled is to look at the value of the VOCERA_SSL environment variable. When VOCERA_SSL is set to ON, SSL is enabled.

> **Important:** If you have a Vocera Voice Server cluster, you should create a new SSL certificate on the standby node(s) first, and then create a new certificate on the active node.

To create a new SSL certificate when it has expired:

1. On the Vocera Voice Server machine, choose Start > All Programs > Administrative Tools > Services to open the Services console.

2. Stop the Apache2 and Tomcat services. Leave the Services console open.

3. In the `\apache\apache2\bin` folder on the Vocera Voice Server, run `cert.bat`.

   This batch file creates a new self-signed certificate named `server.crt` in the `\apache\apache2\conf\ssl` folder. The certificate is valid for 1825 days (5 years) from the creation date. You can verify the expiration date of the certificate by opening the certificate file.

4. In the Services console, start the Apache2 and Tomcat services.

5. Close the Services console.

Report Server IP Address

Learn about the importance of dual registration for Vocera Report Server and Vocera Voice Server.

When you use the Vocera Report Server, it downloads system usage statistics from the Vocera Voice Server daily. This information includes user names, group and department names, frequency of use, and so forth.

To prevent unauthorized access to your data, you must register the IP addresses of the Vocera Voice Server and the Vocera Report Server with each other:

- In the Vocera Voice Server Administration Console, enter the IP address of the Vocera Report Server in the Report Server IP Address field on the System|License Info page.
- In the Vocera Report Server, enter the IP address of the Vocera Voice Server in the **Vocera Voice Server IP Address** field on the Administration|Server Info page.

This dual registration prevents an unauthorized Vocera Report Server from downloading Vocera Voice Server data simply by specifying its IP address.

Monitoring Badge Activity

The Administration Console includes a Badge Status Monitor that displays information about how badges are being used.

This information can help you identify and solve problems. The Badge Status Monitor shows who is logged in, what IP address is currently assigned to each badge, what activity the badge is currently engaged in, whether the badge is in Do Not Disturb or Hold mode, and the current location and site of each user. The Vocera Voice Server updates the Badge Status Monitor at a specified interval.

Similarly, the Group Status Monitor page of the Administration Console displays the name of every group and the number of currently logged in users who are immediate members of that group. If you expand one of the groups, the Group Status Monitor displays columns of information for each of the members. This is the same information that appears in the Badge Status Monitor, except it is sorted by group.

Displaying Vocera Documentation

You can display Vocera documentation online through the Administration Console.

Vocera documentation includes manuals in PDF (Portal Document Format) files and context-sensitive help.

Displaying Documentation Online

The Adobe Reader, a free software program from Adobe Systems Incorporated, is required to display the Vocera documents installed as PDF files.

You can download the Adobe Reader or learn more about it on the **Adobe Reader** home page.

Use the following steps to view the Vocera documentation:

1. Click **Documentation** on the navigation bar.
   The Documentation page displays links to PDF versions of Vocera documents.
2. Click a link to view a document.
   The manual or instruction sheet opens in a separate window.

Displaying Help

The Administration Console provides context-sensitive help.

To display help, click the ? button on any console page.

Sites and Locations

This section describes how to manage sites and access point (AP) locations in your environment.

- Working with Multiple Sites on page 33
- Working with Locations on page 41

Working with Multiple Sites

Learn about Vocera support for multiple physical locations.

In Vocera, a *site* is a logical division of a single Vocera database that corresponds to a distinct physical location. When you create multiple sites, you allow a centralized Vocera Voice Server or cluster to support multiple physical locations whose users can all communicate with each other. You associate users, groups, and other Vocera entries with specific sites to improve speech recognition and to simplify data management.

> **Note:** You can also support multiple physical locations by using a separate, independent Vocera Voice Server or cluster for each physical location. Because these deployments do not utilize sites, badge users in different locations cannot call each other directly–they must use the telephony interface to communicate. Such deployments may be desirable in situations where a high-speed WAN link between each location is not available.

For example, suppose your organization wants to provide badges to users in three physical locations: New York, Philadelphia, and Washington. You can support these users with either of the following deployments:

- A *multi-site* deployment, with one Vocera Voice Server or cluster and individual New York, Philadelphia, and Washington sites.

  This deployment utilizes sites and allows badge users to communicate directly with each other.
- A *multi-server* deployment, with a separate Vocera Voice Server or cluster for each physical location.

  This deployment does not utilize sites or allow badge users to communicate directly with each other. The Vocera Voice Servers operate independently and are not connected.

Use the Sites screen in the Administration Console to define and manage site settings. When a site and the Vocera Voice Server are in different time zones, you can use the Administration Console to specify a time zone for the site.

> **Note:** Do not configure site settings if your installation has only one physical location–by default, all Vocera data is associated with a special site named Global. Similarly, do not configure site settings if you have a multi-**server** deployment.

If you are deploying one Vocera Voice Server to support multiple sites, site configuration is very important. Each site that you define contains its own users, groups, locations, address book entries, and devices. You can set up all your users and groups in the Global site, then transfer them to individual sites later when you define them. It may be more convenient, however, to define your sites in advance and assign users and groups to their appropriate home sites.

A multi-site deployment provides seamless device connectivity across multiple physical locations —users can communicate with other users, groups, and address book entries at their local site as well as at any other site. If users roam from site to site, the Vocera Voice Server knows which site they are visiting and can direct calls to their devices at that site.

Groups, locations, and address book entries at different sites can have the same name. For example, each site can have its own "Front Desk" or "Code Blue" group, its own "Cafeteria" location, and its own address book entry for "The Local Pharmacy".

If you do not want to associate a user, group, address book entry, or device with a specific site, you can assign it to the Global site—a virtual site that does not represent any physical location. For example, you can set up a Global Administrators group with members from each of the individual physical sites.

> **Note:** Partitioning a deployment into multiple sites improves speech recognition. See **Site Grammars** on page 205 for complete information.

Site Terminology

Learn about the different sites you can have in your environment defined by Vocera.

Vocera uses the following terminology to refer to the sites at your installation:

* The *home site* is the usual physical site of a user, group, location, address book entry, or device. See **About the Home Site** on page 34.
* The *current site* identifies the physical site where a user is currently located. See **About the Current Site** on page 34.
* The *Global site* is a virtual site that does not correspond to any physical site. You can assign users, groups, locations, address book entries, or devices to the Global site if you do not want to associate them with a physical site. See **About the Global Site** on page 35.

About the Home Site

Every user, group, location, address book entry, and device has a home site associated with it.

The home site represents a slightly different notion for each of these entities:

Table 8: Home site for different Vocera entities

For this entity...	The home site represents...
User	The physical site where he or she typically works.
Group	The physical site where its members typically work. The members of a group may be from different home sites; however, the group itself is still associated with a home site.
Location	The physical site where its access point is installed.
Address book entry	The physical site of the users who typically call it.
Device	The physical site where the device is located.

You can optionally specify a home site when you create one of these entities. If you do not explicitly specify a home site, Vocera assigns one as described in **Using Site Filters** on page 36. The home site of each user, group, location, address book entry, and device appears in lists throughout the Administration Console to help you identify the entity.

About the Current Site

The current site of a user is the physical site where he or she is located at any given time.

Because users can roam from one physical location to another, their *current* site may be different from their *home* site. The current site of a location, group, or access point is always the same as its home site.

In most situations, a user's current site and home site are identical. A user's current site changes only when the user visits another physical site. You can examine the current site of all users logged into the Vocera Voice Server by viewing the Badge Status Monitor page, as described in Monitoring Badge Activity on page 30.

About the Global Site

Every installation of the Vocera Voice Server has at least one site—the Global site.

Vocera automatically creates the Global site. You cannot create or delete the Global site manually; however, you can perform any other maintenance to it. For example, you can transfer users to and from the Global site, delete groups in the Global site, and so forth.

You can use the Global site in either of the following situations:

- If you do not implement multiple sites, Vocera automatically associates all your entities with the Global site.
- if you do implement multiple sites, but you do not assign certain users, groups, locations, or address book entries to a specific home site, Vocera automatically assigns them to the Global site.

When you upgrade from a version of Vocera that did not include site support, or when you load data with a .CSV file that does not specify site information, Vocera automatically assigns all your entities to the Global site.

If you are not going to implement multiple sites, leave all your data assigned to the Global site. If you are going to implement multiple sites, you can transfer data from the Global site to one or more individual sites. See Transferring Site Data on page 38.

> **Important:** By default, every access point on your network is associated with the Global site. If your deployment implements multiple sites, you must assign a location name to each access point and associate each of these locations with a site. Otherwise, the Vocera Voice Server always thinks that the Global site is your current site.

Calling Between Sites

Users in a deployment with multiple sites can place their most common calls as they always do.

To call a user who is at their current site, or to call a user whose home site is the *same* as their current site, they can simply use their normal voice commands.

However, calling users, groups, or address book entries at *any arbitrary* site is a two-step process:

1. Explicitly connect to the home site or current site of the person you are calling. For example:
   Connect to *Santa Cruz*.
2. Issue a voice command as you normally do. For example:
   Call *April Buckley*.

Similarly, if you are logging in at a site you are visiting you must connect to your home site first:

1. Press the Call button, then wait to hear the log-in prompt.
2. Connect to your *home* site. For example:
   Connect to *Santa Cruz*.
3. When you hear the next log-in prompt, log in by saying or spelling your name as usual. For example:
   April Buckley

If you did not log out before you left your previous site, your badge will roam and automatically connect you to the site you are visiting.

See the "Communicating with Multiple Sites" chapter in the *Vocera Badge User Guide* for complete information about using sites in voice commands.

Using Site Filters

Most pages in the Administration Console have a **Site Filter** field you can use to specify whether to display the data for all sites or for one specific site.

The value that you specify in the **Site Filter** persists until you change it or log out of the Administration Console.

The **Site Filter** determines the default site that a user, group, location, or address book entry is assigned to during data entry. However, you can change this default value during data entry.

Recording a Name for a Site

When the Genie interacts with users, it often speaks the name of a site.

The Genie can synthesize the necessary name prompts. However, if you record name prompts yourself, the Genie can use them to provide more natural-sounding speech and to avoid mispronunciations.

To record a name for a site:

1. Log in with a badge as a user with system administration privileges. See Permissions for Administrators on page 84 for details.
2. Press the Call button, wait for the Genie to answer, and then say, "Record a name for **site name**." (For example, "Record a name for Manhattan.")

   The Genie will prompt you to record the site name prompt.

   Note: If multiple sites, users, groups, locations, and address book entries have the same name or alternate spoken name, you can record a name prompt for only one of them.

Managing Site Information

The Sites screen allows an organization with multiple physical sites to share a single, centralized Vocera Voice Server.

Note: Do not configure site settings if your installation has only a single physical location.

Adding or Editing a Large Number of Sites

Learn how to import site information to a spreadsheet to update a large amount of data.

When you add a site, you specify its name and a basic description only. You need to specify the users, groups, locations, address book entries, and devices that are associated with it separately.

To save time when adding a large number of sites, import them directly from a CSV (comma separated value) file to the Vocera database.

When you add or edit a site, Vocera prompts you for the following basic information.

Table 9: Site fields

Field	Maximum Length	Description
Site Name	50	Enter the name of the site in the Site Name field.
		The name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed.
		By default, the speech recognition system uses the name you enter to recognize sites. If users refer to a site by something other than the name you enter here, enter that name in the Alternate Spoken Name field.
		If you change the name of a site that has a Vocera SIP Telephony Gateway associated with it, you must set the value of the VOCERA_SITE environment variable on the telephony server machine to the name of the new site.
Description	100	(Optional) Enter a description of the site in the Description field.
Alternate Spoken Site Name	50	(Optional) Use the Alternate Spoken Site Name field to enable Vocera to recognize variations of the exact site name.
		For example, if users commonly refer to a site by a nickname or an acronym, enter that variation here.
Cost Center	100	(Optional) Use the Cost Center field to specify a cost center for the site.
Emergency Broadcast Group	n/a	(Optional) Use the Emergency Broadcast Group field to specify the name of the group that receives emergency broadcasts for this site.
		You also set an emergency group for each functional group in your organization. For more information, see **Emergency Broadcast Groups** on page 241.
Time Zone	n/a	(Optional) Use the Time Zone field to specify a time zone for the site. By default, a site's time zone is the Vocera Voice Server's time zone.
		Note: This field does not appear in the data-loading template.
Initiate Emergency Broadcast Silently	n/a	Specifies whether to initiate emergency broadcasts at this site silently, without playing a chime first. This option is available only if a group is specified in the Emergency Broadcast Group field at the site and group. By default, it is unchecked.
		Note: This field is not available for Groups on Add/Edit Group dialog box. A silent emergency broadcast is configured at the **site level only** and will apply to all emergency groups for the entire site including panic groups set per group.
Spoken Name Count	n/a	The Spoken Name Count field displays the total number of names that can possibly be used in a voice command for this site. It includes the names of users, groups, sites, locations, address book entries, and all possible alternate names, such as spellings of user names and the singular and plural names of groups.
		Note: This field contains a display-only value, and it does not appear in the data-loading template.

To Add or Edit a Site

Learn the steps for updating site information.

1. Click Sites in the navigation bar.
2. Click the Sites tab to display the Sites page.
3. Click Add New Site to add a new site, or choose a site name from the list and click Edit Site to edit an existing site.

   The Search for Site option can help you find a site name quickly. As you type a name, Search for Site finds the closest match in the list.
4. Enter information to define the site.

5. When you are finished, take one of the following actions:
    - Click Save to save site data and return to the Sites page. Changes apply as soon as you save them.
    - Click Cancel to return to the Sites page without saving changes.
    - When you are adding a site, you can also click Save & Continue to save site data and begin adding another site.

Deleting Sites

Learn how to delete a site.

When you delete a site, Vocera permanently removes it, as well as all the users, group, locations, address book entries, and devices that are associated with it. Because deleting a site removes all its associated entities, you typically do not delete a site without transferring some of its entities to another site, as described in Transferring Site Data on page 38.

For example, suppose the company you work for is closing the Mountain View office, but all the employees are being relocated to the Cupertino office. You would transfer the users from the Mountain View site to Cupertino before deleting the Mountain View site.

You can delete a site at any time. To ensure that no call activity is interrupted by the changes you make, however, the deletion will not take effect until the system has no calls or Genie sessions in progress.

To delete sites:

1. Click Sites in the navigation bar.
2. Click the Sites tab to display the Sites page.
3. Select one or more sites to delete.

    To select two or more adjacent rows on the Sites tab, click the first row, then hold down SHIFT while you click the last row to select.

    To select two or more nonadjacent rows on the Sites tab, click the first row, then hold down CTRL while you click other rows to select.

    To search for the site name instead, begin typing it in the Search field. As you type, a drop-down list appears with up to 10 matching names. Select one, or click Search to go to the first match.
4. Click Delete Site.

    A warning appears, reminding you that all users, groups, locations, address book entries, and devices associated with the site will be deleted.
5. Click OK.

Transferring Site Data

You can transfer any combination of users, groups, locations, address book entries, and devices from one site to another.

For example, if your organization has closed its New York office and is relocating some employees to the Philadelphia office, you can transfer those users from the New York site to the Philadelphia site.

Similarly, if you have been working with a single site installation of Vocera and are now expanding to support multiple sites, you can transfer your existing users, groups, locations, address book entries, and devices from the default Global site to one of the new sites you are creating.

Vocera prevents you from transferring a group or location in the source site that already has the same name as a group or location in the destination site. Vocera transfers all the other entities you specified and then indicates that errors occurred, as described later in this section.

The home site of a group and the home sites of its members are not necessarily the same. Consequently, transferring a group to a different site does not automatically transfer its members.

Note: When you transfer users to a new site, the Badge Status Monitor immediately displays their new site in the Current Site column, even if the users are still physically located at the original site. When the users reboot their badges, the Badge Status Monitor displays their new current site.

When you transfer site data, Vocera prompts you for the following information.

Table 10: Transfer fields

Field	Description
Site to Transfer From	Click the Select button next to Site to Transfer From, select the site from the list that appears, then click Finish.
Site to Transfer To	Click the Select button next to Site to Transfer To, select the site from the list that appears, then click Finish.
Transfer	Specify the data to transfer: • To transfer all the data from the source site, check All. Groups and locations in the source that already exist in the destination will not be transferred. • To transfer only some of the data from the source site, check Selected, then click the Select button to display the Select Transfer Entities dialog box, then specify the data to transfer. See **Select Transfer Entities** on page 39 for more details.

When you transfer users to a new site, the Badge Status Monitor immediately displays their new site in the Current Site column, even if the users are still physically located at the original site. When the users reboot their badges, the Badge Status Monitor displays their new current site.

To transfer site data:

1. Click Sites in the navigation bar to display the Sites page.
2. Click the Transfer tab to display the Transfer page.
3. Enter required information.
4. Click Transfer.

   Vocera transfers your data and displays a dialog box showing you the progress. When the transfer is finished, Vocera displays the progress as 100%.

   If Vocera cannot transfer all the data successfully, it transfers as much data as possible and displays the Show Errors button in the Progress dialog box.
5. If necessary, click Show Errors to review errors in your import. When you are finished, click OK to close the Errors dialog box.
6. Click OK to close the Progress dialog box and return to the Administration Console.

Select Transfer Entities

The Select Transfer Entities dialog box lets you select any combination of users, groups, locations, address book entries, and devices in the source site for transfer to the target site.

The Select Transfer Entities dialog box appears when you click the Select button in the Transfer section of the Site Transfer page.

To select the data that you want to transfer:

1. Check the types of entities that you want to transfer.

   The names of the individual entities appear in the list box.

   For example, suppose you want to transfer some of the users and groups from one site. When you check the Users and Groups boxes, the list box displays the names of all users and groups associated with the source site.
2. Select the specific items you want to transfer in the list box.
   • To select a single item, click its name.
   • To select multiple items, hold down the Ctrl key as you click each name.

- To select a range of items, click the first name in the range, then hold down the Shift key and click the last name in the range.

3. Click Finish.

   The Select Transfer Entities dialog box closes, and the items you selected appear in the Transfer section of the Site Transfer page.

Working with Locations

Locations are names of places to which you assign one or more access points.

When a badge connects to an access point, the Vocera Voice Server is able to report the corresponding location. The location names also appear in the Badge Status Monitor, replacing the MAC address of the access point.

The **Locate**, **Where Is?**, and **Where Am I?** voice commands allow users to find the physical location of a particular user or member of a group within a site. If you configure locations for your system, the Genie can respond with information about a user's whereabouts ("Roswell Adams is near the First Floor Cafeteria," for example). If you do not configure locations, the Genie will answer with the MAC address of the access point instead, which is not useful to most badge users ("Lucy Crysek is near access point zero zero four zero nine six four five B D four E," for example).

> **Important:** By default, every access point on your network is associated with the Global site. If your deployment implements multiple sites, assign a location name to each access point and associate each of these locations with a site. Otherwise, the Vocera Voice Server always thinks that the Global site is your current site.

To configure locations, it is important that you:

- Use a map of your facility to define the physical boundaries of your locations, and note which access points fall within the boundaries of each.
- Enter location names in the Locations page of the Administration Console, and choose neighbors for each location.
- Assign one of the pre-configured locations to each access point. You can do this in the Administration Console, but the easiest way to assign locations is to do a Walking Tour using the badge.

After you create locations, you can define adjacent or nearby locations as *Neighbors*. When a user issues a command to locate the nearest group member, the Vocera Voice Server searches only the current location of the requester, plus the locations you have defined as neighbors. Thus, the system uses neighbors to determine who is nearest to a particular location.

However, the badge, like other wireless devices, does not always associate with the access point that is physically closest. Depending upon building construction, a badge can associate with an access point situated on a different floor. The badge can only offer approximate user locations; consequently, general location names may be more useful than specific ones.

Defining Locations

To define locations, use the Locations page in the Administration Console.

Before you begin, obtain a map of the facility and note where the access points are installed. (This may already have been done as part of the site survey performed before the Vocera system was installed.)

Based on the physical layout and access point coverage, you can draw boundaries and assign location names to different areas of the facility. You can then refer to this map when configuring locations in the Administration Console.

Location information will be most accurate if you draw the boundaries around sizeable, contiguous areas. Vocera badges, like most wireless devices, remain connected to a particular access point as long as the signal is acceptable, even if the user moves closer to a different access point. As a result, a user who crosses the boundary of one location may still be connected to an access point that is located in an adjacent location. If you choose well-defined locations, such a wing of a large building or a floor of a smaller building, you minimize the effects of the signal retention.

After you create the location map, you can add locations and choose their neighbors in the Vocera Administration Console. Then you can record a name prompt for each location. (See Recording a Location Name on page 42.)

Recording a Location Name

When you record a name using your natual voice, it can avoid mispronunciations.

When the Genie interacts with users, it may need to speak the name of a location. The Genie can synthesize the necessary name prompts. However, if you record name prompts yourself, the Genie can use them to provide more natural sounding speech and to avoid mispronunciations.

To record a name prompt for a location:

1. Log in with a badge as a user with system administration privileges. See Permissions for Administrators on page 84 for details.
2. Press the Call button, wait for the Genie to answer, and then say, "Record a name for *location name.*" (For example, "Record a name for the Cafeteria.")
   The Genie will prompt you to record variations of the location name.

   Note: If multiple sites, users, groups, locations, and address book entries have the same name or alternate spoken name, you can record a name prompt for only one of them.

Access Point Location Information

Learn about assisgning a name to each access point in your enviroment to easily identify the location of team members.

A *location* is the common name of the place where an access point is located. For example, a location may be a name such as Break Room or 6 North.

After you assign location names to access points, you can use the names in voice commands (Find a member of nurses close to the E R), and the Genie responds with location names when appropriate (Art Lacrosse is near the Main Desk). The location names also appear in the Badge Status Monitor, replacing the MAC address of the access point.

To configure locations, use the Locations screen in the Administration Console. Before you begin, obtain a map of the facility and note where the access points are installed. (This may already have been done as part of the site survey performed before the Vocera system was installed.)

Based on the physical layout and access point coverage, you can draw boundaries and assign location names to different areas of the facility. You can then refer to this map when configuring locations in the Administration Console.

   Note: When you need to add a large number of locations, you can save time by importing them directly from CSV files to the Vocera database. See Importing Data from a CSV File on page 162.

Adding and Editing Locations

Learn the steps for adding and editing the names of access points.

Use the Add/Edit Location dialog box to create new locations and modify existing locations.

To add or edit a location:

1. Click Locations in the navigation bar.
2. On the Locations page, click Add New Location to add a new location, or choose a location name from the list and click Edit Location to edit an existing location.

    The Search for Location option can help you find a location name quickly. As you type a location name, Search for Location finds the closest match in the list.

    The Add/Edit Location dialog box appears.
3. Enter or edit the information required on the Info tab.

    See **Location Information Page** on page 43.
4. Optionally enter or edit the information required on the Access Points tab.

    See **Access Points Page** on page 44.
5. Enter or edit the information required on the Neighbors tab.

    See **Neighbors Page** on page 44.
6. Click Save & Continue to save this location and begin to add another, or click Save to save this location and return to the Locations page.

Location Information Page

The Location Information page of the Add/Edit Location dialog box (or the corresponding fields in the data-loading template) lets you specify basic information about a location such as its name, description, and site, as well as an alternate spoken name.

Enter the following information in the Location Information page of the dialog box:

Table 11: Location information fields

Field	Maximum Length	Description
Location Name	50	Enter a Location Name. The name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed. By default, the speech recognition system uses the name you enter to recognize locations. If users refer to a location by something other than the name you enter here, enter that name in the Alternate Spoken Location Name field.
Description	100	Optionally enter a Description to help you identify the location on the Locations page.
Site	50	Use the Site field to specify the physical site of the access point. In the Add/Edit Location dialog box, click the Select button to open the Select Site dialog box, then choose a name from the list and click Finish. • If your organization has multiple sites connected to the same Vocera Voice Server, choose the site that represents the access point's physical location. • If your organization does not have multiple sites, accept the default Global setting. When working in the data-loading template, leave this field blank to accept Global.

Field	Maximum Length	Description
Alternate Spoken Location Name	50	Enter an Alternate Spoken Location Name, if needed.
		By default, the name in the Location Name field is used for voice recognition. When a user says the name of a location (" Locate members of managers closest to the first floor, " for example), the Vocera Voice Server software matches the speech with the text in the Location Name field.
		If the location has an unusual name (for example, if a building is named after a person and that person has a name that is not spelled the way it is pronounced), enter the name the way it sounds when it is pronounced out loud, rather than the way it is actually spelled.
		You may also want to enter an alternate spoken location name if the location is commonly called by an unofficial name (if the Administration Building is often called the "Clock Tower Building," for example). The Alternate Spoken Location Name gives the server an additional field to check, increasing the chances that a location name will be understood by the Genie.

Access Points Page

The Access Points page of the Add/Edit Location dialog box lets you assign the name of the location you are creating to one or more access points.

You can manually enter the MAC address of each access point on this page, or you can specify the MAC addresses in either of the following ways:

- Use a badge and voice commands to assign location names to the access point your badge is currently associated with while you roam.

  This method is recommended, because it is easier and less error-prone than entering MAC addresses. See Using Voice Commands to Assign Access Points on page 45.
- Use the access points data-loading template to associate MAC addresses with each location. See the *Vocera Data-Loading Reference*.

To assign MAC addresses to the location name manually:

1. Click the Access Points tab to display the Access Points page.
2. The Access Points page of the Add/Edit Location dialog box displays a list of access point MAC addresses for a location. You can add or delete items from the list.

   - To add an address, click Add to display the Add Access Point MAC Address dialog box. In the MAC Address field, enter the MAC address (12 hexadecimal characters) of an access point that you want to assign to this location, then click Finish. The address appears in the list of access point addresses.

     To specify a range of MAC addresses that have the same first 11 characters, enter "0" for the 12th character. The "0" character is treated as a wildcard only in the 12th character of the MAC address.

   - To delete an address, choose a MAC address from the Access Point Addresses list, then click Delete.

Neighbors Page

You can add neighbors individually for each location and define search limits on a location-by-location basis.

When someone uses a Locate command for a group ("Locate the nearest Supervisor," for example) the Vocera Voice Server searches the requester's current location and all of its neighboring locations, but no other locations.

Note: Voice commands to locate an individual ("Locate Mary Benham" or "Where is Mary Benham?") will always return the location of the individual at the current site. To locate an

individual at a different site, you must first connect to that site using the "Connect to *Site*" command.

Choose neighbors that are adjacent to or otherwise physically near the location you are configuring. If the Locate voice command will be used to find the nearest emergency worker, for example, it is not advisable to define a very broad search area.

Before you can associate locations with neighbors, the neighbors must themselves be added as locations. In practice, this means that you cannot always add neighbors when you add a location.

- If you could not add neighbors when you added a location, you will need to edit the location. To do this, select the location in the Add, Edit, and Delete Access Point Locations page and click Edit Location. In the Edit Location dialog box, click the Neighbors tab.
- If you are in the process of adding a location, click the Neighbors tab in the Add Location dialog box.

To add neighbors to a location:

1. Click the Add button in the Neighbors page of the Add/Edit Location dialog box. The Select Location dialog box appears, showing all locations that have been added to the system.
2. Select the locations you want to add as neighbors.
    - To select multiple locations, hold down the Ctrl key as you click each location.
    - To select a range of locations, click the first location in the range, and then hold down the Shift key as you click the last location in the range.
    - To quickly find a location on the list, begin entering the name in the Search field. As you type, the system finds the closest match.
3. Click Finish. The neighbors you selected appear in the list on the Neighbors tab.
4. Click Save. You are now ready to assign access points to the location.

Using Voice Commands to Assign Access Points

Learn the steps for adding a new access point to a location in your enviroment.

In the following procedure, you will use the *Begin Tour*, *End Tour*, and *Assign Location* voice commands to assign access points to locations.

Before you begin:

- If possible, make a map that shows the boundaries of the locations you have chosen for your facility, as well as the position and MAC address of each access point.
- In the Administration Console, create all of the locations you need by completing the required fields in the Location Information tab. You can also associate locations with Neighbors during this process.
- Make sure you are logged in to your badge as a member of a group with the Perform System Administration permission.
- You can use voice commands on a badge to assign access points to locations only when you are at your home site.

To assign access points to locations:

1. Using a badge, log in to the Vocera system.
2. Press the Call button. When the Genie answers, say "Begin Tour."
    The Genie confirms that you are beginning your tour, and then you hear a tone that signals that the Genie has bowed out. The Vocera Voice Server is still monitoring your movements over the wireless network, however.
3. Begin walking slowly through the area covered by your network. Each time your badge connects to a new access point, the Genie returns and announces the MAC address or location of the access point.

4. After announcing a MAC address, the Genie asks if you want to assign a location. Stop walking, and then say the name of the location you want to assign to the new access point.

> **Important:** The location name must be one that you already configured in the Administration Console.

If the Genie announced the name of the location, it means the access point is already assigned to that location, and the Genie bows out. If you want to change the location assignment, press the Call button, say "Assign Location" and then say the name of the location when prompted.

5. Continue walking and assigning locations until you have assigned all of the access points to locations.

6. When you have finished assigning access points to locations, say "End tour."

You can check whether a location is being reported accurately without starting another tour. To do this, press the Call button, wait for the Genie to answer, and then say "Where am I?" If you need to change the location name, use the *Assign Location* command.

Deleting Locations

Learn the steps for deleting a location.

To delete a location:

1. Click Locations in the navigation bar to display the Add, Edit, and Delete Access Point Locations page.

2. Select one or more locations to delete.

   To select two or more adjacent rows on the Locations tab, click the first row, then hold down SHIFT while you click the last row to select.

   To select two or more nonadjacent rows on the Locations tab, click the first row, then hold down CTRL while you click other rows to select.

   To search for the location instead, begin typing it in the Search field. As you type, a drop-down list appears with up to 10 matching names. Select one, or click Search to go to the first match.

3. Click Delete Location.
   A message asks you to confirm the deletion.

4. Click OK.

Users, Groups, and Permissions

This section describes how to manage users, groups, and permissions.

Managing Users

Adding new users to the system and updating information for existing users are two primary tasks of a Vocera system administrator.

The Users screen lets you add, edit, and delete user profiles.

When you add a user (or when a user self-registers), the Vocera system creates a *profile* for that user in the Vocera Voice Server database.

You can use any of the following methods to add user profiles to the Vocera system:

- To manage one user profile at a time, work with the Users page in the Administrations Console.
- To save time when adding a large number of users, import them directly from a CSV (comma separated value) file to the Vocera database.
- To allow users to add themselves via the User Console, see Allowing Users to Register Themselves on page 51.

After a user has had some time to work with the badge, you may need to edit the user's profile to add features that may be useful or remove features that the user does not want. In addition to a user's name and contact information, the profile stores user preferences, such as which Genie persona will prompt the user, whether warning tones are played when the badge has a low battery, or when the user has a new voice or text message.

Before You Add Users

Learn the considerations and necessary tasks to perform prior to creating the users in your environment.

Complete the following tasks before you add users to the system:

1. If necessary, create individual sites so you can select them when you create each new user.
   Create individual sites only if your Vocera system supports users at multiple physical locations. Otherwise, leave the Site field blank and Vocera will assign the user to the Global site automatically.
2. Create departments and other groups so you can select them when you create each new user.
3. Develop a systematic method for assigning a unique user ID to each user. Users enter their own user IDs to access the User Console, and they enter the user IDs of other users to send an email message from a mail client to a badge.
   Here are some possible methods for assigning user IDs:
   - Make them the same as existing employee ID numbers.
   - Make them the same as existing email addresses, but without the domain reference. For example, if a user's email address is *zrohina@yourcompany.com*, the user ID could be *zrohina*.

- Combine the initial of the first name and the full last name of a user to create a user ID. For example, if a user's name is *zami rohina*, the user ID could be *zrohina*.

  You can use any combination of alphanumeric values to create a user ID. Pure alphabetic values are typically easier for users to remember. However, in certain situations, you may need to use numeric or alphanumeric values for user IDs.

  For example, Vocera uses the user ID as a PIN to uniquely identify users to a nurse call management system. if you are integrating Vocera with a nurse call management system that requires numeric or alphanumeric PINs, you can provide these values as user IDs.

4. When you enter names into the system, use the character set of the locale. For example, Celine would not be pronounced the same way in French as Céline. It may therefore be necessary to add alternate spoken names (for example, "Sailine") or new dictionary entries.

Enabling Login/Logout Voice Commands

Voice commands for logging in and out from a badge are enabled and disabled via the Preferences page of the System screen in the Administration Console.

The commands work like this:

- When Login/Logout Voice Commands are enabled and no one is currently logged in when you power up a badge, the badge prompts you to say or spell your first and last name.

  The system logs you in when you respond to this prompt. The screen of the badge then displays your name, and your user profile is updated to reflect the Badge ID (MAC address) of that badge.

- If you are already logged in to a badge, the screen displays your name. If you press the Call button and say "Log out," the system removes you as an active user and deletes the Badge ID from your user profile. The screen on your badge then displays "Logged Out."

If users share badges, you should enable Login/Logout Voice Commands.

If each user is permanently assigned a badge, you may wish to disable Login/Logout Voice Commands. In this case, you must manually set the Badge ID for each user in the Edit User dialog box on the Users page of the Administration Console.

Recording Name Prompts for a User

If you record a name for a user, the recorded name is played when the Genie needs to say the user's name; for example, when the user logs in, when the Genie confirms a call to the user, and when a call is announced.

If a user does not have a recorded name, the Vocera Voice Server uses its text-to-speech software to announce the user's name. Your system can process only a certain number of text-to-speech operations at one time. To ensure that users do not experience delays, you may want to record users' names as you add the individuals to the system. You can then encourage the new users to record their names in their own voices when it is convenient for them.

To record a name prompt for a user:

1. Log in with a badge.
2. Press the Call button, wait for the Genie to answer, and then say, "Record a name for *user's name.*" (For example, "Record a name for Mary Hill.")

   Note: If multiple sites, users, groups, locations, and address book entries have the same name or alternate spoken name, you can record a name prompt for only one of them.

   The Genie will prompt you to record variations of the user's proper name.

About Users and Telephone Numbers

If your site has the telephony integration option enabled, entering telephone numbers for users provides a wide range of connectivity between Vocera devices (badges and smartphones), on- and off-site telephones, and pagers.

You can provide any of the following telephone numbers when you add users to the Vocera system:

Table 12: Vocera telephone number fields

Telephone Number	Description
Desk phone or extension	Allows a user to forward or transfer calls from a Vocera device to a desk phone. If the Vocera Extension field is filled in, the Desk Phone Or Extension field is used only for forwarding. Otherwise, this number is also used for the following purposes: • Direct dialing from smartphone keypads • Paging callbacks • Vocera hunt number access You can also use the Dynamic Extension feature to assign extensions to users. See the *Vocera Telephony Configuration Guide* for more information.
Cell phone	Allows a user to forward calls from a Vocera device to a mobile phone.
Home phone	Allows a user to forward calls from a Vocera device to a home phone. It also allows a user to take advantage of the "Call My House" address book entry.
Pager	Allows a user to receive calls on a pager from other Vocera users who issue the "Page" voice command.
Vocera Extension	Allows a user to route calls made to a virtual extension to their Vocera device instead. This field is useful for users who do not have actual desk extensions, or users who have both a Vocera smartphone and a desk phone. The Vocera Extension field takes precedence over the Desk Phone or Extension field for the following purposes: • Direct dialing from smartphone keypads • Paging callbacks • Vocera hunt number access You can also use the Dynamic Extension feature to assign extensions to users. See the *Vocera Telephony Configuration Guide* for more information.

If you do not enter values for these numbers, the Genie informs users who try to access these features that the number is not available.

You must set permissions to allow users to forward calls to telephones and to allow users to have toll or toll-free pager numbers.

Choosing Between Vocera Extensions, Desk Phones, or Dynamic Extensions

Learn the different types of extensions and phones user's can be configured to connect with.

Each user can be configured to use one of the following phone numbers to route outside calls and calls made from the smartphone keypad to their Vocera device:

• Vocera Extension
• Desk Phone or Extension
• Dynamic Extension

Both the Vocera Extension and Desk Phone or Extension fields can be filled in, but the Vocera Extension field takes precedence for direct dialing, paging callbacks, and Vocera hunt number access. When the Vocera Extension field is filled in, the Desk Phone or Extension field is used only for forwarding.

Dynamic extensions are artificial telephone numbers that Vocera associates with users automatically, on an as-needed basis, if they need a number to enable a paging call-back on badges or smartphones. You can use dynamic extensions in either of the following situations:

• Vocera users do not have actual desk extensions and you want Vocera to assign an extension to users automatically.

• You are using Direct Inward Dialing (DID) extensions for Vocera devices, but you don't have enough DID numbers to dedicate one to each Vocera user.

For information about configuring dynamic extensions, see the *Vocera Telephony Configuration Guide*.

> **Note:** The Data Check page of the Administration Console lets you check whether users have been assigned the same Vocera extension. For more information, see **Checking Data** on page 169.

DTMF Matching

Learn about Dual-tone multi-frequency signaling (DTMF) in the Vocera environment.

By default, when someone dials an extension after calling the Vocera hunt group number, or types a number on a smartphone, or calls a Vocera DID number, the Vocera system attempts to match the number with one of the following numbers in the Vocera system in this order of priority:

• A user with a matching Vocera Extension

• A user with a matching Desk Phone

• A user with a matching Dynamic Extension

• A group with a matching Vocera Extension

• A matching broadcast sequence

  For example, the prefix for urgent broadcasts (666 by default), followed by a group Vocera Extension.

If there is no match of the number in the Vocera system, the dialed number is sent out to the PBX.

Allowing Users to Register Themselves

When you check Self Registration in the Preferences page of the System tab in the Administration Console, people can use the User Console to add themselves to the Vocera system.

Each person who registers is given one of the available user licenses.

1. Specify permissions for the "Everyone" group and the defaults that you want to assign to all users. After users register, they can change their announcement settings and other options.

2. Enable Self Registration on the Preferences page. To do this, click System in the navigation bar, click the Preferences tab, and then check Self Registration.

3. Assign the user IDs yourself. To make user IDs more predictable, it is best to give users the user IDs you want them to have, rather than allow them to create user IDs themselves.

4. Give new badge users the User Console URL, and tell them to click the Register button.

   The User Console URL is http://*vocera_machine_name*/console/index.jsp, where *vocera_machine_name* is the name or IP address of the Vocera Voice Server.

5. Tell users that all names they enter in the User Console must begin with a letter or digit. They must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed.

About Temporary Users

A temporary Vocera user is a user account that expires at the first system sweep that occurs following a date that you specify.

When a temporary user account expires, Vocera deletes all information about the user from the database, and the user can no longer log in. See Setting Sweep Options on page 111.

Because unnecessary user accounts increase the size of the speech recognition space significantly, you should always delete them. Temporary users simplify maintenance because Vocera automatically deletes them when they are no longer necessary. See The Dynamic Grammar on page 204 for complete information about how user accounts increase the size of the recognition space.

Use the Add/Edit User dialog box to create a temporary user. See Adding or Editing a User Profile on page 52 for more information.

Generic User Profiles

A *generic user profile* is a user name that you add to the Vocera database with a person's role instead of with the person's first and last name.

For example, the names "Temp Nurse One" and "Manager on Call" are both generic profiles if they are configured as *users*. Multiple people typically use a generic user profile to log in at different times, instead of only a single person.

Generic user profiles hinder or defeat the following Vocera features:

- Personal messages

  Users cannot leave personal messages for an individual who is using a generic profile. Anyone using the profile can listen to the message and delete it.

- Learned names and commands

  Individual users can train the Genie to recognize the way they say names and commands. When multiple users share a single profile, the system learns the way one person speaks, but the other users will have bad speech recognition and may be unable to place basic calls.

- Asset management

  When a badge is lost, the Vocera Report Server helps you find it by identifying the last user that logged in with it. When the most recent user is a generic profile, you cannot determine which person last used the missing badge.

- Call by name

  You cannot call a person with a generic profile by name, locate that person, or even find out if he or she is on site.

Vocera recommends that you avoid creating generic user profiles because they interfere with basic badge usage and unintentionally cause user confusion. Instead, set up roles as *groups*, use first and last names to configure user profiles, and then assign users to a role by adding them to the appropriate group. Individual badge users then have access to all Vocera features, and callers can find them by using either their names or roles.

Adding or Editing a User Profile

Learn the steps for editing a user profile in the Adminstration Console.

Use the Add/Edit User dialog box to create or edit a user. Individual pages in the Add/Edit User dialog box let you specify different types of information about the user you are creating or editing.

Information in a user profile is organized into the following categories. Each category has its own page in the Add/Edit User dialog box.

- Basic User Information on page 53
- User Phone Information on page 55
- Speech Recognition on page 57
- Group Membership on page 58
- Department List on page 59

To add or edit a user profile:

1. Click Users in the navigation bar.
2. Click Add New User to create a user profile, or choose a user name from the list and click Edit User to edit an existing user profile.

   The Search for User option can help you find a user name quickly. You can search by typing last name, first name, and user ID in any order in the Search field. As you type, autocomplete assists by displaying the closest match in drop-down menu that appears below the Search list.

   > **Note:** If you enter user information proceeded by a comma, the autocomplete feature no longer displays predicted search results.

3. The Add/Edit User dialog box opens. Add or edit data as appropriate.
4. After working with a page in the dialog box, do one of the following:
   - Click Save to save changes, close the Add/Edit User dialog box, and display the Users page.
   - Click Save & Continue to save the user profile and leave the Add/Edit User dialog box open to add or edit another user.
   - Click another tab in the Add/Edit User dialog box to enter additional user information.

Basic User Information

The User Information page of the Add/Edit User dialog box (or the corresponding fields in the data-loading template) lets you specify basic information about a user such as a user name, user ID, and password, as well as accounting information such as an employee ID and cost center ID.

Table 13: Basic user information fields

Field	Maximum Length	Description
First Name, Last Name	50	Enter the user's First Name and Last Name in the corresponding fields. The name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed. By default, the speech recognition system uses the names you enter to recognize users. If people refer to a user by something other than the name you enter here, provide an Alternate Spoken Name in the Speech Recognition tab.
User ID	50	Enter a User ID that is not already assigned to another user on the system, being careful to choose a name that you and the user can easily remember. The user ID is not case-sensitive. The User ID must contain only letters, digits, spaces, periods (.), underscores (_), or dashes (-). No other characters are allowed. It must not begin or end with a space. Note: You must have System Administrator or Tiered Administrator permissions to change or enter the User ID.
Employee ID	50	Optionally use the Employee ID field to specify a unique value that identifies a Vocera user. Note: You must have System Administrator or Tiered Administrator privileges to change or enter the Employee ID.

Field	Maximum Length	Description
Password	25	Optionally enter a Password of five to 25 characters for the user, and re-enter the password to make sure you typed it correctly. Letters, digits, spaces, periods, dashes (-), asterisks (*), and underscore characters (_) are allowed. The password is case-sensitive. If Vocera authentication is used, the password is required for tiered administrators, and Staff Assignment users. It is not required to access the User Console. If Active Directory authentication is enabled for the Vocera Voice Server, the Vocera password is not required. If you have specified an Initial User Password on the Passwords page of the System screen, Vocera automatically adds it to a profile that has a blank password after you save the profile. Initial user passwords do not affect *existing* user profiles, only profiles that you create after specifying the initial password. **Note:** This field does not appear in the data-loading template.
Email Address	60	Enter the user's email address to take advantage of these features: • Other users can send voice messages from their badges to this user's email inbox. Vocera sends voice messages to an email address as .WAV file attachments. Users can listen to these messages with the Windows Media Player and other players. • The Vocera system administrator can send the user an email from the Administration Console with instructions on how to install and configure Vocera Connect. • The Vocera system administrator can integrate the user with Vocera Messaging Platform (VMP). If so, enter a unique email address. Otherwise, theVMP Server will not synchronize the user successfully. **Note:** To enable email features, you must also configure the settings on the Email page of the Administration Console.
Site	50	Use the Site field to specify the user's home site. In the Add/Edit User dialog box, click the Select button to open the Select Site dialog box, then choose a name from the list and click Finish. • If your organization has multiple sites connected to the same Vocera Voice Server, choose the home site that represents the user's physical location. • If your organization does not have multiple sites, accept the default Global setting. When working in the data-loading template, leave this field blank to accept Global.
Cost Center	100	Optionally specify a value in the Cost Center field. A cost center ID lets Vocera track system usage by users and potentially allows an organization to charge for relative usage.
Badge ID	12	Enter the MAC address of the user's badge in the Badge ID field as follows: • If the system-wide setting Login/Logout Voice Commands is *enabled*, you do not need to enter the Badge ID, because it will be entered automatically when the user logs in. • If Login/Logout Voice Commands is *disabled*, use the Info menu on the badge to find the Badge MAC address, and enter this address in the Badge ID field. The MAC address of a badge is also printed near the bottom of the white label under the battery.
Temporary User	n/a	Optionally allows you to create a temporary Vocera user account. The first message sweep that occurs after midnight on the expiration date automatically removes a temporary user account. You should always delete user accounts that are not necessary. When a temporary user expires, Vocera deletes all information about the user from the database, simplifying maintenance for the system administrator. **Note:** This field does not appear in the data-loading template.

Field	Maximum Length	Description
Expiration Date	n/a	Specifies the last full day that a temporary user account is available. The first message sweep that occurs after midnight on this date automatically removes the temporary user. This field is required if you check the Temporary User field. When a temporary user account expires, all information about the user is removed from the Vocera database, and the user can no longer log in. Select an expiration date by clicking the calendar icon to the right of the field, or type the date in the field. If you type the date, use the correct date format: United States: `mm/dd/yyyy` Other locales: `dd/mm/yyyy`

User Phone Information

The Phone page of the Add/Edit User dialog box (or the corresponding fields in the data-loading template) lets you provide telephone numbers and additional phone-related information for each user. If your site has the telephony integration option enabled, entering telephone numbers for users enables connectivity between the badge, on- and off-site telephones, and pagers. If you do not enter values for these numbers, the Genie informs users who try to access these features that the number is not available.

Table 14: User phone information fields

Field	Maximum Length	Description
Desk Phone or Extension	50	Enables the following features: • Allows users to forward or transfer calls from their Vocera devices to their desk phones. • If no Vocera Extension is specified, allows outside callers to connect to a user's Vocera device by entering the user's desk extension at the Vocera hunt group prompt, instead of saying the user's name. • Allows users to send a page and receive the return phone call from a person they paged on their badges. • If users have appropriate permission and have Vocera Access Anywhere enabled, the Desk Phone or Extension field allows users to be authenticated by Caller ID when they call the Vocera hunt group number.
Cell Phone	50	Allows users to forward calls from a badge to a cell phone. If users have appropriate permission and have Vocera Access Anywhere enabled, the Cell Phone field allows users to be authenticated by Caller ID when they call the Vocera hunt group number.
Home Phone	50	Allows users to forward calls from their badges to their home phones. It also allows users take advantage of the "Call My House" address book entry.
Pager	50	Allows users with the proper permissions to receive numeric pages on their pagers from other badge users who issue the "Page" voice command.
Vocera Extension	50	Allows a user to route calls made to this virtual extension to go to their Vocera device instead. If the Vocera Extension field is filled in, it is used for • Direct dialing from smartphone keypads • Paging callbacks • Vocera hunt number access If you leave this field blank, smartphone users and outside callers can dial the user's desk phone to be routed to the user's Vocera device. Because the Vocera extension is a virtual phone number, you can put any number in the Vocera Extension field. If a user already has a desk phone number, you can reuse that number for the Vocera Extension field but prepend a digit, such as 8, to make the number unique in the Vocera system. Vocera extensions are not constrained by fixed-length numbers for your PBX. You can also enter DID numbers for Vocera extensions.
Dynamic Extension	50	As Vocera assigns dynamic extensions, they appear in this read-only field. Because dynamic extensions are assigned on-demand, this field may be empty even after you enable the dynamic extensions feature. Similarly, this field will continue to display an expired number that has not been reassigned; the user keeps the number as long as it is available. See the *Vocera Telephony Configuration Guide* for more information.
PIN for Long Distance Calls	50	Allows an organization to authorize or account for telephone usage and to distribute telephone costs among different users, departments, or sites. A PIN template can include digits, special characters, and PIN macros.

Field	Maximum Length	Description
Cisco EM Extension	n/a	If Vocera Connect for Cisco has been deployed and Cisco Extension Mobility has been enabled, you can use this read-only field to verify whether Extension Mobility is assigning the right phone number to the user for Vocera calls.
Cisco EM Auto-Answer	n/a	If Vocera Connect for Cisco has been deployed and Cisco Extension Mobility has been enabled, you can use this read-only field to verify whether Extension Mobility is assigning the right phone number to the user for Vocera broadcasts and urgent messages.
Enable Vocera Access Anywhere	n/a	When this option is checked, the user can access the Genie from a telephone to perform Vocera functions other than basic calling. The number of users that can use the Vocera Access Anywhere feature is controlled by your Vocera license. If you check this box, make sure you enter a Phone Password for all users that are not authenticated by Caller ID when they access the Genie from a phone. **Note:** This field does not appear in the data-loading template.
Phone Password	25	Password used to authenticate the user when accessing the Genie from a phone. The Phone Password must be five to 25 characters consisting of letters or numbers. Special characters are not allowed. Do not enter your regular Vocera password that you use to log into the User Console. Note: This field does not appear in the data-loading template.
Re-Enter Phone Password	15	Retype the same password you entered in the Phone Password field. Note: This field does not appear in the data-loading template.

You must set permissions to allow users to forward calls to telephones and to allow users to have toll or toll-free pager numbers.

Speech Recognition

The Speech Recognition page of the Add/Edit User dialog box (or the corresponding fields in the data-loading template) lets you provide variations of a user's name or identifying phrases to assist in speech recognition.

Table 15: User speech recognition fields Field Maximum Length Description

Field	Maximum Length	Description
Alternate Spoken Names	50	Specify variations of the user's name in the Alternate Spoken Names fields. The name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed. **Note:** Even though the characters listed above are allowed, it is unlikely that an alternate spoken name would need underscores (_), or dashes (-). • If users refer to a person or place in various ways, enter each variation in a different field. For example, enter `Bob Jones` and `Rob Jones` in addition to `Robert Jones`. Similarly, enter a nickname that the person or place is known by, such as `Skip Jones.`. • **Important:** It is recommended that you do not create an alternate spoken name that contain numeric digits only. For example, a staff ID with numbers and no letters: `567748` Entering numeric staff IDs is permitted. However, the possible results of using numeric values only is: • Slower Genie response time • Problems with phone number recognition • If people use initials to refer to a user, provide them as a series of letters separated by spaces. For example, if users refer to Amardeep Munindar Gill as A.M. Gill, enter `A M Gill`. • If a name has an unusual or confusing pronunciation, enter a name that is spelled as it is pronounced. For example, if the system does not recognize the name *Jodie Dougherty*, you could enter `Jodie Dockerty`. • If users refer to a person by his or her title, provide the full spelling of the title. For example, enter `Father Brown` instead of `Fr. Brown`.
Identifying Phrase	100	Optionally specify an Identifying Phrase to help Vocera distinguish this user from another whose first and last names are spelled the same. For example, if there are two users named Mary Hill on the system, but one is on the third floor and the other is on the first floor, you could enter `Mary Hill on the third floor` as the identifying phrase for one user and `Mary Hill on the first floor` for the other.
Enable Frequently Called User	Not applicable	Optionally select the check box next to Enable Frequently Called User to enable this feature for individual users.

Group Membership

The Assign User to Groups page of the Add/Edit User dialog box lets you specify the groups each user belongs to.

Note: You cannot add members to or remove members from the built-in Everyone group. The Vocera Voice Server maintains membership in the Everyone group automatically.

To specify group membership:

1. Add the user to a group by clicking Add, selecting the group name or names from the list that appears, and clicking Finish.
   The groups appear in the Group Name list. Vocera indicates the permissions resulting from group memberships as check marks in the Permissions list.
2. Remove the user from one or more groups by selecting the groups and clicking Delete.
   The names are removed from the Group Name list.

Department List

The Departments page displays the list of departments a user belongs to. You cannot add a user to a department directly—Vocera determines department membership according to the groups that users are assigned to. That is, if a user is a member of a group, and that group has the Group Type property set to Department, then the user is also a member of that department. If a user is a member of a group and that group has the Group Type property set to Subdepartment, then the user is also a member of any parent department group(s).

Vocera populates the Departments page when you save the user profile. If you are creating a new user and assigning that user to groups, you will not see any information in the Departments list until you save the user profile.

When you *export* users to a `.csv` file, Vocera populates this field for informational purposes. When you *import* users through the data-loading template, any value in this field is ignored, because you cannot assign department membership directly.

Deleting Users

When you delete a user from the system, that person's profile is expunged from the system, and the person's name will no longer be recognized.

You can delete a user at any time. To ensure that no call activity is interrupted by the changes you make, however, the deletion will not take effect until the system has no calls or Genie sessions in progress.

To delete users:

1. Click the Users button on the navigation bar to display the Add, Edit, and Delete Users page.
2. Select one or more users to delete.

   To select two or more adjacent rows on the Users tab, click the first row, then hold down SHIFT while you click the last row to select.

   To select two or more nonadjacent rows on the Users tab, click the first row, then hold down CTRL while you click other rows to select.

   To search for the name, using any order enter the last name, first name, or user ID in the Search field. As you type, a drop-down list appears with up to 10 matching names. Select one, or click Search to go to the first match.

   Note: If you enter user information proceeded by a comma, the autocomplete feature no longer displays predicted search results in the drop-down list.

3. Click Delete User.

   A message asks you to confirm the deletion.
4. Click OK.

User Console Overview

The User Console is a browser-based application that enables users to display and edit profile information and settings stored on the Vocera Voice Server .

The User Console provides additional capabilities, such as the ability to create buddies, forward calls, send text messages to badge users, and manage groups. Users can log in to the User Console from any computer that meets the criteria specified in Browser Requirements on page 21.

The User Console URL is either of the following:

* `http://vocera_ip_address/console/index.jsp`
* `https://`vocera_ip_address`/console/index.jsp`

where `vocera_ip_address` is the numeric IP address of the Vocera Voice Server .

To learn more about the User Console, see the *Vocera Voice Server User Console Guide*. You can also log in to the User Console and click the ? button on any page.

Editing User Data on the User Console

You can login into the Vocera User Console as an Administrator and update a user's information.

To edit User Console data for a user:

1. Open the User Console. The main login page opens.
2. On the main login page, enter the following:
    a. In the **User ID** field, enter the user's user name.
    b. In the **Password** field, enter your Administrator password.
3. Click **Login**. The Vocera User Console opens.
4. Navigate to desired screen and make the needed changes.

For more information about logging into the User Console, see the *Vocera User Console Guide* .

Vocera Access Anywhere

If a telephony integration option is installed with your Vocera system, you can use a standard phone to call the Vocera hunt number to direct the call to any Vocera user, group, or Address Book entry.

This section describes how to configure your Vocera system so that users can access the Genie from a standard phone and use many of the same voice commands available from a badge.

> **Important:** The Vocera Smartphone provides a Vocera client within a WiFi phone. You can use the Vocera Smartphone to call other Vocera users directly without first calling the Vocera hunt number.

Types of Access to the Genie

Learn the ways you can access the Vocera Genie using hunt numbers.

When you use a phone to call the Vocera hunt number for a site, there are two types of access:

- **Guest access** – Callers can interact with the Genie to place a call. They are not identified to the called person and cannot issue voice commands. This type of access requires no additional configuration or user licenses, and it is the same type of access that existed prior to Vocera 4.1.
- **Direct access** – Once callers are authenticated, either by Caller ID or by name and password, they have full permission to access the Genie to issue Vocera commands. This type of access is enabled by user license and requires configuration in the Vocera Administration Console.

Only specifically enabled users can use a phone to call the Vocera hunt number and then access the Genie to issue voice commands. These users may not have a badge or may need to access Vocera commands remotely, for example, from their cell phone.

Vocera Access Anywhere Licensing

Vocera Access Anywhere requires a special Vocera license key.

Vocera Access Anywhere is a feature that is included with Vocera SIP Telephony Gateway. The license key determines the number of users that can be enabled to use the feature. To obtain additional user licenses for Vocera Access Anywhere or a Vocera SIP Telephony Gateway license, please contact Vocera.

Administering Vocera Access Anywhere Licenses

To see how many Vocera Access Anywhere licenses you have to distribute to users, click System in the navigation bar to display the System screen.

For more information, see Displaying License Information on page 106.

You can specify that new users are enabled for Vocera Access Anywhere by default, and you can also override current user settings to enable Vocera Access Anywhere for all users. For more information, see Choosing Miscellaneous Settings on page 121.

Important: If you use the system default to enable Vocera Access Anywhere and also override current user settings, you may eventually use all available Vocera Access Anywhere user licenses. When all available Vocera Access Anywhere user licenses are being used, you cannot add new user profiles to Vocera until you disable the Enable Access to Genie from Phone default.

You can generate an Administration Console report of all users that have been enabled for Vocera Access Anywhere. The report helps you manage your Vocera Access Anywhere licenses. For more information, see Generating Reports on page 202.

Guest Access and Direct Access Numbers

Learn the ways you can access the Vocera Genie using hunt numbers.

When you configure Vocera SIP Telephony Gateway there are two Vocera hunt group numbers you can specify:

- Guest Access – This number is for guest access to the Vocera system. However, users enabled for Vocera Access Anywhere can call the Guest Access number and then press star (*) to be authenticated and start a Genie session.
- Direct Access – This number is for specially licensed user access to the Vocera system. This field is used only if your Vocera system has a digital or IP connection to the PBX, you have selected an ISDN or SIP signaling protocol, and Calling and Called Party Information is enabled on the PBX. Vocera uses the Caller ID feature to automatically authenticate users when they call the Direct Access number from their desk phone or cell phone.

These Vocera hunt group numbers should be coordinated with your PBX administrator.

Enabling Vocera Access Anywhere

There are several steps to enable Vocera users to access the Genie from their phones.

When you enable users, you must decide how they are going to authenticate themselves to the system. For more information, see the following sections:

- Authenticating Users by Caller ID on page 63
- Authenticating Users by Password on page 63

To enable Vocera Access Anywhere for a user:

1. In the Administration Console, click Users in the Navigation bar.
2. Select a user, and then click Edit User. The Add/Edit User dialog box appears.
3. Click the Phone tab.
4. Make sure the Enable Vocera Access Anywhere checkbox is checked.
5. If you are using Caller ID to authenticate the user, make sure the Desk Phone or Cell Phone fields have a number.
6. If you are using the name and phone password to authenticate the user, make sure the Phone Password and Re-enter Phone Password fields have been completed. The phone password must be between 5 and 15 characters consisting of letters or numbers. Other special characters are not allowed.
7. If you are using Caller ID to authenticate the user:
   a. Create a group named "Access Vocera Anywhere Using Caller ID".
      For information on how to create a group, see Adding or Editing a Group on page 74.
   b. Grant the following permission to the group:

- Access Vocera Anywhere Using Caller ID

  For information on how to grant permissions to group members, see Group Permissions on page 79.

c. Add members to the group.

  For information on how to add group members, see Group Members on page 77.

8. The user can now call one of the Vocera hunt numbers from a phone to access the Genie.

   - If you are using Caller ID to authenticate users, they can call the Direct Access number for direct access to the Genie.

   - If you are using the name and phone password to authenticate users, they can call either the Guest Access or Direct Access number, and then press star (*) key to access the Genie.

Authenticating Users by Caller ID

If your telephony integration uses ISDN or SIP signaling protocol and Calling and Called Party Information is enabled on the PBX, you can use the Caller ID feature to automatically authenticate users when they call the Direct Access number from their desk phone or cell phone.

To authenticate users using Caller ID, make sure the user belongs to a group with the Access Vocera Anywhere Using Caller ID permission. For more information, see Special Permissions on page 236.

When a user calls the Direct Access number, here is how authentication works:

- If the user has the Access Vocera Anywhere Using Caller ID permission, and he calls from a phone number that is stored in his Vocera user profile, the user immediately hears the Genie prompt.

- If the user does not have the Access Vocera Anywhere Using Caller ID permission, the Genie prompts for the user's first and last name, and then prompts for his phone access password. See Authenticating Users by Password on page 63.

> **Note:** Users can also access the Genie by calling the Guest Access number. When users call the Guest Access number, the Genie says, "Good morning. Say the full name of the person or group you want to reach or enter an extension." At that point, users can initiate a Genie session by pressing the star (*) key.

Authenticating Users by Password

Learn how to access a user via the Genie using a password.

When users call the Guest Access number, the Genie says, "Good morning. Say the full name of the person or group you want to reach or enter an extension.". At that point, users can initiate a Genie session by pressing the star (*) key. They are then prompted to say their first and last name, and then to enter their phone access password followed by the pound (#) sign.

Vocera Access Anywhere Special Keys

If the Genie requires a yes or no response, you can press 1 for "Yes" or 2 for "No."

You can also press 2 to cancel a command. For example, if you are calling someone and you change your mind, press 2 to cancel the action.
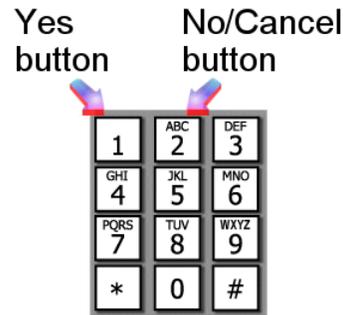
Figure 5: Special phone keys for Vocera Access Anywhere

> **Important:** Because Vocera uses the 1 and 2 keys for its functionality, it does not fully support calling Interactive Voice Response (IVR) phone numbers while you are accessing the Genie from a phone.

Testing Vocera Access Anywhere

This section describes how to test whether Vocera Access Anywhere is working properly.

To verify that users can access the Genie from a phone:

1. If Caller ID authentication is supported, make sure the Access Vocera Anywhere Using Caller ID group is set up correctly.

   a. In the Administration Console, open the Access Vocera Anywhere Using Caller ID group.

   b. Click the Permissions tab and verify that the following permission is granted:

      - Access Vocera Anywhere Using Caller ID

      > **Note:** You should grant the Access Vocera Anywhere Using Caller ID permission only if your Vocera system has a digital or IP connection to the PBX, you have selected an ISDN or SIP signaling protocol, and Calling and Called Party Information is enabled on the PBX. Otherwise, the permission has no effect.

   c. Click the Member tab and add your user name to the list of group members.

   d. Click Save to save the group.

2. Make sure your user profile is configured to enable access to the Genie from a phone.

   a. Open your user profile, and click the Phone tab.

   b. Make sure the Enable Vocera Access Anywhere checkbox is checked.

   c. If you are testing authentication using Caller ID, enter a phone number in the Desk Phone or Cell Phone fields.

   d. If you are testing authentication using a phone password, enter a Phone Password. The password must be 5 to 15 characters.

   e. Click Save to save changes.

3. If Caller ID authentication is supported, test it:

   a. Call the Direct Access number from your desk phone or cell phone.

   b. You should be automatically authenticated based on your Caller ID. The Genie says, "Good morning, [FirstName]. [Chime] Vocera."

   c. Try to call another Vocera user. For example, "Call *John Smith*."

   d. To disconnect the call, press 1 or hang up the phone.

4. Test name and password authentication:

   a. Call the Guest Access number from a phone other than the desk phone or cell phone entered in your user profile.
   The Genie says, "Good morning. Say the full name of the person or group you want to reach or enter an extension."

   b. Press the star (*) key. This causes the Genie to switch to direct access mode.

The Genie prompts you to say or spell your first and last name.

c. Say or spell your first and last name.

The Genie prompts you to enter your phone access password followed by the pound sign (#).

d. Enter your phone access password followed by the pound sign (#).

The Genie says, "Good morning, [FirstName]. [Chime] Vocera."

You can now say a Vocera command.

Working with Groups and Departments

The Groups screen displays the group name and home site for all groups in the site you specify with the Site Filter field.

An asterisk (*) next to the name of a group indicates that it is a department. Two asterisks (**) next to the name of a group indicates that it is a subdepartment.

If you have the View Users and Groups permission, the View All Groups checkbox at the bottom left of the page is enabled. Otherwise, it is disabled. When View All Groups is checked, you can view all groups in the selected site, not just groups that you manage. System administrators always view all groups, so the View All Groups checkbox is disabled for them.

Vocera groups organize users into roles such as Floor Manager, Cashier, Nurse, Cardiologist, Executive, and so forth. Groups provide different features to different members of an organization:

- To the administrator, groups provide a streamlined way to manage user permissions based on their roles.
- To the badge user, groups provide a way to communicate with users based on their roles.
- To the organization itself, groups provide a way to direct and forward call traffic based on user roles.

Group membership can change over time, and in some environments it can change frequently. A user can be a member of multiple groups at the same time. An administrator can add and remove group members either with voice commands or through the Administration Console. Users can remove themselves from groups, and if you enable the proper permission, they can add themselves or other users to groups.

About Group Properties and Permissions

When you create or modify a group, you specify values for properties that control the way the group behaves and the way users interact with it.

Groups provide a way to leave messages for many users at once ("Send a message to Nurses Assistants"), or to call someone who fits a specific role ("Call a sales person"), belongs to a certain department ("Call Accounts Receivable"), or has some other skill or authority that the caller requires ("Call a manager").

The following list summarizes the properties available in Vocera groups:

- *Identification* properties specify the group name and contact information.
- *Speech recognition* properties specify the names that users can speak to call a group, and the names that the Genie can use to prompt users.
- *Scheduling* properties specify how calls are routed to members when users call a group.
- *Department* properties determine whether a group is used as a department, and optionally specify a telephony PIN or Cost Center ID for accounting purposes.
- *Membership* properties define the set of users who are members in a group and the order in which Vocera routes calls to them, if you specify the round robin scheduling option.

- *Forwarding* properties determine the flow of calls from one group to another, potentially through your entire organization.
- *Permissions* determine the ability of users to issue certain commands or perform specific operations.
- *Conference* properties determine which users are in an instant "push-to-talk" conference that simulates the behavior of a walkie-talkie.

In some situations, it is useful to include a group as a member of another group. For example, in a health care environment, you may want the Nurse group to include the Head Nurse and Charge Nurse groups. In this example, Head Nurse and Charge Nurse are *nested groups*.

The permissions that you specify for a group flow down to the members of any nested groups. For example, if the Communications group is nested within the Marketing group, the members of Communications receive the permissions that you specify for Marketing, unless you revoke a specific permission for Communications.

While it is often beneficial to nest groups to establish permissions and call flows, it is usually better to avoid nesting groups that are used as departments.

About Groups and Sites

Groups are associated with a home site, which represents the home site where the users in the group typically work.

For example, cardiologists who work at the Society Hill site could belong to a group called Cardiology whose home site was also Society Hill.

Members of a group do not have to belong to the same site, however. For example, you could create a Cardiology group with members from the Society Hill site, the West Philadelphia site, and the Old City site. In this situation, you typically assign the Cardiology group to the Global site to indicate that its members span multiple sites.

If you are not working in a multi-site deployment, you must associate all your groups with the Global site.

Group Managers

Every group that you create can be managed by members of a different group.

For example, a member of the Charge Nurse group may need to manage the Code Blue group in a hospital, or a member of the Head Cashier group may need to manage the Cashier group in a retail store.

Members of a group with management capabilities can perform any of the following tasks for the groups they manage:

- Change all of the basic information except the group name and the site.
  The basic information includes alternate spoken names and other speech recognition features, scheduling options, and the group phone extension.
- Specify whether to use the group as a department, enter a PIN for telephony, and enter a cost center ID.
- Add and remove group members, change their order, and specify whether the group has only temporary membership.
- Change the forwarding options.
- Specify a group whose members can add themselves to the managed group.
- Maintain the list of members in the associated conference group.

Group managers can use the Administration Console or User Console to change and review group capabilities. Group managers do not have system administration permission. Only a system administrator can create a group, delete it, or assign permissions to it. See System Administrators on page 25 for additional information.

> **Tip:** To allow group managers to view all groups on the Groups and Group Status Monitor pages of the Administration Console, grant them the View Users and Groups permission. Otherwise, they will only be able to view groups that they manage on those pages.

Members of a group with management capabilities can also use voice commands to add and remove members from the managed group. For example, a member of the Head Nurse group that manages the Code Blue group could say "Add Lin Ma to Code Blue." See the *Vocera Badge User Guide* for more information.

Group Device Managers

The devices owned by a group or department can be managed by members of a different group.

For example, a member of the Cardiology Device Managers group may need to manage the devices owned by the Cardiology group in a hospital.

Group device managers can use the Administration Console to perform any of the following tasks for the groups they manage:

- View the Badge Status Monitor and Device Status Monitor to monitor the status of devices currently connected to the network.
- View the Devices tab for groups whose devices they manage.
- Modify Label, Owner, Site, Status, Shared Device?, and Notes fields for a device.

The group you assign to manage the devices of a group can be the same group that manages the group, or you can create a separate group of device managers. The group of device managers does not require any additional permissions.

Groups with Temporary Membership

When the membership of a group is dynamic, you may want to specify that it contains only temporary members.

For example, suppose a hospital uses a **Code Blue** group to respond to patient emergencies. Membership in this group changes with every shift, and membership also changes from day to day—that is, users who are in **Code Blue** on Monday are not necessarily members of the group on Tuesday.

Groups with such requirements can cause a maintenance problem, because users typically forget to remove themselves from the group at the end of their shifts. Temporary membership solves this problem, because Vocera automatically removes users from the group when they log out, while leaving them in the database. Users are *not* added into the group automatically when they log back in.

To minimize maintenance, you typically specify a separate group of users who can add themselves to the group with temporary membership. Users can then add themselves to the temporary group at the beginning of their shifts, and have Vocera remove them automatically at the end of the shift. For example, you can specify that members of the **Nurses** group can add themselves to the **Code Blue** group.

Check the Remove Users on Logout box on the Member page of the Add/Edit Group dialog box to specify that membership in the group is temporary. Use the Group of users permitted to add themselves to this group field on the Permissions page of the same dialog box to specify a group whose members can add themselves to the group with temporary members. See Adding or Editing a Group on page 74 for complete information.

> **Note:** Users are only removed from the group when they log out. Keep in mind that users may place badges in the charger or simply leave the site without logging out when their shifts end. To accommodate this behavior, consider enabling the following options:

- The Auto Logout When Badge In Charger setting. See Choosing Badge Notifications on page 119.
- The Enable Auto-Logout Period setting. See Setting System Preferences on page 109.

About the Built-In "Everyone" Group

Whenever you add a new site to the system, Vocera automatically creates an **Everyone** group for that site.

Vocera automatically creates and maintains a special group called **Everyone** for each of your sites:

- If you have a single-site deployment, Vocera maintains the **Everyone** group for the Global site.
- If you have a multi-site deployment, Vocera maintains a separate **Everyone** group for each physical site as well as an Everyone group for the Global site.

When you create or delete a user, Vocera adds or removes that user from the appropriate **Everyone** group automatically. By default, the Groups tab in the Administration Console displays an **Everyone** group for each of your sites.

You cannot delete an **Everyone** group, add members to it, remove members from it, add an Emergency Broadcast Group to it, or change the site it is associated with—only Vocera maintains these features. You can, however, specify all the other properties for an **Everyone** group, such as its call forwarding properties, its scheduling, and its permissions. An **Everyone** group is a special group—the Vocera administrator creates and deletes all other groups through the Administration Console.

The order of names in a group affects the group scheduling properties, which determine how calls are routed. Because Vocera automatically adds new users to the *end* of the **Everyone** group, you may want to manually rearrange this order to optimize scheduling.

The **Everyone** group determines the default set of permissions for the users at its site.

The "Everyone Everywhere" Group

Vocera also creates an **Everyone Everywhere** group when you complete your installation or upgrade.

Each **Everyone** group is a member of **Everyone Everywhere**.

Like an **Everyone** group, Vocera automatically maintains membership in **Everyone Everywhere**, but you can specify all other properties for it. Unlike the **Everyone** group, there is only one **Everyone Everywhere** group, and it is associated with the Global site.

The **Everyone Everywhere** group determines the default set of permissions for users across all sites.

About the Built-In VST Groups

After you install or upgrade the Vocera Voice Server, the VSTContacts and VSTUsers groups are created in the Global site to allow a potential integration with the Vocera Secure Texting solution.

- If the database of the Vocera Voice Server contains data (that is, during an upgrade), the groups VSTContacts and VSTUsers are created immediately.
- If the database of the Vocera Voice Server is empty (that is, during a new installation), the groups VSTContacts and VSTUsers are created as soon as you create a user or a group in the Vocera Voice Server.

See the *VST Hospital Administrator Guide* for complete information.

About the "Operator" Group

You can optionally create a group named **Operator** and populate it with members—either groups or users—who are always available, such as store operators or the front desk.

Vocera provides quick access to an **Operator** group for callers who dial the Vocera hunt group or DID number. If a caller enters **0** (for Operator) when prompted by the Genie, Vocera directs the call to the **Operator** group. If you specify a forwarding number for the Operator group, you can redirect the call if no group member is available. For example, you can forward calls to the **0** extension on your PBX.

Recording a Name for a Group

if you record name prompts yourself, the Genie can use them to provide more natural sounding speech and to avoid mispronunciations.

When the Genie interacts with users, it often speaks the name of a group. For example, the Genie speaks the name of a group or the singular member name when it prompts users who call the group to leave a message for group members. The Genie can synthesize name prompts for a group.

> **Note:** If multiple sites, users, groups, locations, and address book entries have the same name or alternate spoken name, you can record a name prompt for only one of them.

To record a name for a group:

1. Log in on a badge as a user with system administration privileges or as a member of a group with management permission for this group. See Group Device Managers on page 68 and Permissions for Administrators on page 84.
2. Press the Call button, wait for the Genie to answer, and then say, "Record a name for *group name.*" (For example, "Record a name for Nursing.")
   The Genie will prompt you to record variations of the group name.

About Groups and Departments

A *department group*, also called a *department*, is a group that corresponds to a department within the organization using the Vocera system.

By designating a group as a department, you provide accounting features and speech recognition enhancements that are not available to other Vocera groups.

For example, suppose the Midtown Medical Center has units such as ICU, Pediatrics, and Radiology. If your Vocera configuration has corresponding groups, it makes sense to designate those groups as departments. Users at Midtown Medical Center can then take advantage of the extended accounting and speech recognition features of these Vocera departments.

To help you identify a department group, Vocera displays an asterisk (*) next to its name throughout the Administration Console. Similarly, Vocera displays two asterisks (**) next to a subdepartment name.
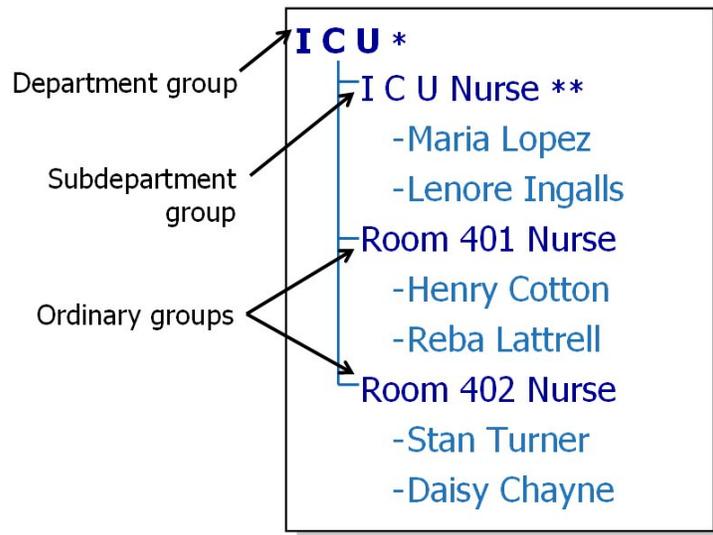
Figure 6: Different types of groups

Sub-departments

A sub-department is a subgroup of a department group and whose members are also considered to be assigned to the parent department group for purposes of departmental calling.

Vocera displays two asterisks (**) next to the name of a group in the Administration Console to indicate that it is a subdepartment.

Sub-department groups, like department groups, are intended to be relatively static. That is, members should not be dynamically assigned to a subdepartment. Only groups that are directly contained within an existing department or sub-department should have their Group Type field set to sub-department. Sub-departments can be nested any number of levels deep within a department.

A sub-department group should be a member of only one parent department. If you make the same sub-department group a member of multiple departments, the Data Check utility will flag the problem and recommend that you remove the sub-department group from all but one department.

Department Membership

Learn the features associated with department membership.

In Vocera, department membership determines the following features:

- Inner circle membership.
- How users can be referenced in voice commands.
- PINs for telephony access.
- The cost center ID.
- The data set used by many of the reports created by the optional Vocera Report Server.

In general, departments provide the greatest benefit when you:

- Do not nest department groups.

  Vocera treats nested departments systematically, as explained below, but users who do not understand that system may perceive unexpected results.

  For example, users may be uncertain about which Vocera department they are in, and which sets of people should show up in various reports created by the Vocera Report Server.
- Make sure all users are assigned to a department.

- Make sure departments are not too large or too small. Departments should have between 3 and 1000 members.

If you do need to create nested departments, Vocera determines department membership as follows:

- Immediate members of a department group are always members of that department. This is true even when the department group is nested under another department group.
- When a department group contains other subdepartment groups, the members of the nested subdepartment groups are members of the nearest department above them.

For example, suppose Pediatrics is a department group that contains the Pediatric Nurses group, and suppose Maddie Hall is an immediate member of Pediatric Nurses.

- If Pediatric Nurses is a department group, Maddie is a member of the Pediatrics Nurses department but *not* the Pediatrics department.

Pediatrics *
    └Pediatric Nurses *
       -Maddie Hall

- If Pediatric Nurses is a sub-department group, Maddie is a member of the Pediatrics department.

Pediatrics *
    └Pediatric Nurses **
       -Maddie Hall

- If Pediatric Nurses is an ordinary subgroup, Maddie is *not* a member of the Pediatrics department.

Pediatrics *
    └Pediatric Nurses
       -Maddie Hall

Make sure you consider any unintentional side-effects if you create nested department groups.

Departments and Accounting

Implementing Vocera departments optionally allows an organization to distribute system usage and telephony costs among different divisions.

Use the following for cost control and distribution of charges:

- A telephony PIN authorizes members of a Vocera department to make phone calls and allows an organization to charge departments for those calls.
- A Cost Center ID enables Vocera to track system usage by department and potentially allows an organization to charge its departments for relative usage.

Departments and Voice Commands

Departments are a convenient way to let badge users contact each other with voice commands.

When a caller specifies a department in a voice command, Vocera can:

- Differentiate among users with the same first and last names.

> For example, if your organization has two individuals named John Smith, a user can issue the voice command "Call John Smith in Tech Support."

- Identify a badge user when the caller knows the first name and department, but not the last name, of other people in the organization.

  For example, a caller can issue the voice command "Call John in Tech Support."

In addition to departments, you can also use identifying phrases to differentiate among users. However, departments are usually easier to set up than identifying names, and more natural for users to work with.

About Call Forwarding

The groups you set up determine the call forwarding that is possible within your organization.

When you create or modify a group, you can specify any of the following call forwarding options:

- No forwarding
- Forward to group pager
- Forward to another badge, group, or address book entry
- Forwarding to an off-network group member
- Forward to another number

The forwarding option you choose determines the action Vocera takes when no member of a group is available to receive a call.

For example, suppose a call—either an internal call from a badge, or an external call, when telephony is enabled—is directed to the Plumbing group in a retail store. If no one in the Plumbing group is available, you may want to forward the call to the Hardware group. Similarly, if no one in Hardware is available, you may want to forward the call to a general group that is always available, such as Customer Support.

Do not confuse the call forwarding options you can specify for a group with the call forwarding options an individual user can specify. Call forwarding for a group determines the call flow through an entire organization; call forwarding for an individual user is more of a courtesy or convenience.

Call forwarding for a group occurs only when a call is directed to a *group* ("Call Plumbing"), not to one of its *members* ("Call Roberta Verdi"). If Roberta Verdi is a member of Plumbing, calls that are placed directly to her are not forwarded to Hardware—her own calls are forwarded according to the options she specifies through voice commands or the User Console. Similarly, when a call is placed to a group, the group properties determine where the call is forwarded, and the forwarding options specified by individual users are ignored.

You can configure Vocera to forward a group's calls to a pager. For example, you may have a "Doctor on call" group that frequently needs calls forwarded to a pager. In this situation, enter a pager number in the Pager field on the Info page of the Add/Edit Group dialog box, and forward the group's calls to the pager.

In addition, you can enable a group forwarding to send calls to a group member who is off-network so that on-call users can receive their calls off-campus or in other off-network environments. If this option is selected, Vocera sends the call to a device that is not in-network or off-campus using the forwarding behavior configured in the Vocera User Console for that user.

About Instant Conferences

The conference feature provides badges with "push-to-talk" communication that simulates the behavior of a walkie-talkie.

Users in a conference can instantly communicate with others in the same conference by pressing and holding the Call button—they don't have to wait for speech recognition or Genie interactions.

The Vocera System Software supports a practically unlimited number of conferences. Many conferences can be active at the same time, with different users in each one. Users within the same conference can interact with one another.

Every group has a conference associated with it. For example, if your site has groups called Managers and Cashiers, users automatically have access to conferences with those names. Although users can be in multiple groups simultaneously, each user can be in only one conference at any time.

Users do not need to be group members to *use* a conference; however, they need the **Conference** permission to *enter* or *leave* a conference. Users can issue voice commands or access the User Console to enter or leave conferences. You can use the Administration Console to assign users to conferences. Group managers can also maintain the user list for the conferences associated with their groups.

Adding or Editing a Group

Use the Add/Edit Group dialog box to create or edit one group at a time. Individual pages in the Add/Edit Group dialog box let you specify different types of information about the group you are creating or editing.

You can change group information at any time. To ensure that no call activity is interrupted, changes take effect as soon as no calls or Genie sessions that affect the group are in progress.

Note: When you need to add a large number of groups or group members, you can save time by importing them directly from CSV files to the Vocera database. See **Importing Data from a CSV File** on page 162.

After you create groups, be sure to record name prompts for them. If you record prompts, the Genie uses them instead of synthesizing names when speaking to users.

To add or edit a group:

1. Click Groups in the navigation bar to display the Groups page.
2. Click Add New Group to create a group profile, or choose a group name from the list and click Edit Group to edit an existing user profile.

   The Search for Group option can help you find a group name quickly. As you type a name, Search for Group finds the closest match in the list.
3. The Add/Edit Group dialog box opens. Add or edit data as appropriate.
4. Do one of the following:
   - Click Save to save changes, close the dialog box, and return to the Groups page.
   - Click Save & Continue to save changes and leave the dialog box open to create another group.
   - Click another tab in the dialog box to enter additional group information.

Basic Group Information

The Info page of the Add/Edit Group dialog box (or the corresponding fields in the data-loading template) lets you specify the group name, its telephone number, alternate names for the group and its members, and scheduling information.

Table 16: Basic group information fields

Field	Maximum Length	Description
Group Name	50	The name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed. By default, the speech recognition system uses the Group Name to recognize groups. If users refer to a group by something other than the Group Name, provide an Alternate Spoken Group Name.
Site	50	Use the Site field to specify the group's home site. In the Add/Edit Group dialog box, click the Select button to open the Select Site dialog box, and then choose a name from the list and click Finish. If your organization has multiple sites connected to the same Vocera Voice Server, choose the home site that represents the member's physical location. If the group's membership spans multiple sites, choose Global. If your organization does not have multiple sites, accept the default Global setting.
Vocera Extension	75	Optionally enter a telephone extension number for the group in the Vocera Extension field. Important: This number is a virtual extension, not an actual desk extension. If the telephony integration option is installed, outside callers who dial the Vocera hunt number can connect to the group by entering the group extension at the Genie prompt, instead of saying the group name.
Pager	75	Optionally provide a pager number for the group in the Pager field. You can configure Vocera to forward a group's calls to this specified pager. If you enter a value for this field, any user can issue the "Send a page" voice command to send a numeric page to this group.
Permission Only (not callable)	n/a	Optionally disable calling and broadcasting to this group by checking this box. Generally, you should disable calling and broadcasting only for administrative groups, that is, groups used to grant or revoke Vocera permissions. All other groups should have calling enabled. Note: You cannot use this field to disable an emergency broadcast to a designated emergency broadcast group. Even if the group is configured to not be callable, members will receive the incoming emergency broadcast call. If you check this box, DO NOT enter a value in the Vocera Extension field for the group. Otherwise, users will still be able to call the group by dialing its extension. Note: Checking the Permission Only box does not prevent permission-only groups from appearing in Vocera smartphone clients even though the groups are not callable. If users have access to the User Console, they can also add a permission-only group to their Buddies list.
Emergency Broadcast Group	n/a	(Optional) Use the Emergency Broadcast Group field to specify the name of the group that receives emergency broadcasts for a functional group. Note: A silent emergency broadcast is configured at the site level only and will apply to all emergency groups for the entire site. For more information, see **Emergency Broadcast Groups** on page 241.
Member Name-Singular	50	In the Member Name-Singular field, enter a name that describes a member of the group. For example, in the group called *Sales*, a group member would be known as a *sales person*. This would allow the Genie to recognize a command such as, "Call a sales person." Best Practice: Do not start the singular name of members with the words "a" or "an" because those words are already in the Vocera grammar.

Field	Maximum Length	Description
Member Name-Plural	50	In the Member Name-Plural field, optionally enter a name that collectively describes the members of the group. For example, in the group called *Sales*, the collection of group members could be called *sales people*. This would allow the Genie to recognize a command such as, "Send a message to all sales people." Best Practice: Do not start the plural name of members with the word "all"—for example, *all sales people*—because that will result in redundant syntax in Genie prompts, such as, "I'm recording a message for **all** sales people."
Alternate Spoken Group Name	50	In the Alternate Spoken Group Name field, optionally enter a variation of the group name. For example, some people might say "the Sales team" instead of "Sales." If you enter *the Sales team* as an Alternate Spoken Group Name, the Genie will recognize "Call the sales team."
Scheduling Options	n/a	Specify either of the following: • Choose Sequential if you want one person to be the main contact. The second member in the list is called only if the first person is not available, a third member is called only if the first two are unavailable, and so forth. The order in which names appear in the Group Member Name list on the Members tab of the Add/Edit Group dialog box is important when you choose Sequential scheduling. • Choose Round Robin if you want calls to be distributed as evenly as possible among group members. When you choose round robin, Vocera iterates through members in the group until someone accepts the call; however, the person who most recently accepted a group call is tried last. If you provide a value other than Sequential or Round Robin in the data-loading template, an error will occur when you try to import the file.
Receive Offsite Calls	n/a	Check this setting to permit calls to the group to be received by members who are currently at a different site from the caller. If your Vocera system has only one site, this option does not apply. If you don't want members to receive calls to the group when they are currently at a different site from the caller (if the site of the group is Global) or at a different site from the group (if the site of the group is not Global), uncheck this setting.
Receive Offsite Broadcast	n/a	Check this setting to permit broadcasts to the group to be received by members who are currently at a different site from the person who initiated the broadcast. If your Vocera system has only one site, this option does not apply. If you don't want members to receive broadcasts to the group when they are currently at a different site from the caller (if the site of the group is Global) or at a different site from the group (if the site of the group is not Global), uncheck this setting.

Department Groups

The Department page of the Add/Edit Group dialog box (or the corresponding fields in the data-loading template) lets you specify the group type (Ordinary, Department, or Subdepartment) and enter a telephony PIN or Cost Center ID for accounting purposes.

The Member Of list shows all parent groups to which the current group is a member.

Table 17: Group department fields

Field	Maximum Length	Description
Group Type	n/a	Select a group type: • Ordinary – a group whose members are NOT considered members of a parent department. Examples of ordinary groups include administrative groups, groups with dynamic membership, role-based groups, and bed/room groups. • Department – a group that corresponds to a department within the organization using the Vocera system. By designating a group as a department, you provide accounting features and speech recognition enhancements that are not available to other Vocera groups. For example, you can differentiate users by specifying their department in voice commands. If you select Department, the PIN for Long Distance Calls and Cost Center fields become editable. • Subdepartment – a subgroup of a department group. Members of a subdepartment are also considered members of a parent department. A subdepartment should be directly contained within an existing department or another subdepartment.
PIN for Long Distance Calls	50	Optionally specify a value in the PIN for Long Distance Calls field. A telephony PIN authorizes members of a Vocera department to make phone calls and allows an organization to charge departments for those calls. A PIN template can include digits, special characters, and PIN macros. Use this field only if you are working with a department group.
Cost Center	100	Optionally specify a value in the Cost Center field. A Cost Center ID enables Vocera to track system usage by department and potentially allows an organization to charge its departments for relative usage. Use this field only if you are working with a department group.

You can also specify a group as a department or subdepartment on the main Departments page that you access through the navigation bar in the Administration Console.

Group Members

The Members page of the Add/Edit Group dialog box lets you add members to and remove members from a group.

You can also make group membership temporary, and change the order in which group members are called when you use sequential scheduling.

If you are working with the data-loading templates, you can perform these same tasks as follows:

• Use the Groups template to specify that membership in a group is temporary.
• Use the Group Members template to add and remove group members, and to specify the order in which group members are called when you use sequential scheduling.

Note: You cannot add members to or remove members from the built-in Everyone group. The Vocera Voice Server maintains membership in the Everyone group automatically.

For convenience, you can also add an individual to a group when you create or edit user information.

Table 18: Group member fields

Field	Description
Group Member Name	Manage membership in any of the following ways: • To add members, click Add Name, select the name or names from the list that appears, and then click Finish. The names appear in the Group Member Name list. • To change the order of a name, select it in the list and click Move Up or Move Down. The ordering of names matters only if sequential scheduling is selected for Scheduling Options on the Info tab. • To remove a member from the list, select it and click Delete Name. Note: This field does not appear in the Groups data-loading template. Use Group Members template to assign members to group and to specify the order of members.
Remove Users on Logout	Check to specify that membership in the group is temporary. When you check this field, Vocera automatically removes users from the group when they log out, but leaves the rest of the user profile in the database. Users are *not* added into the group automatically when they log back in. Important: Users are only removed from the group when they log out. Keep in mind that users may place badges in the charger or simply leave the site without logging out when their shifts end. To accommodate this behavior, consider setting the following options to log users out automatically: • Enable the Auto Logout When Badge In Charger setting. • Check the Enable Auto-Logout Period setting. If you are working in the Groups data-loading template, specify either True or False. If you do not provide a value, False is assumed.

Forwarding Options

The Forward page of the Add/Edit Group dialog box (or the corresponding fields in the data-loading template) lets you specify forwarding options for the group.

The Genie uses the forwarding option when no members of a group are available to take a call.

Table 19: Group forwarding fields

Field	Maximum Length	Description
No Forwarding	n/a	No Forwarding means that if a call to the group is not answered, the caller is prompted to leave a message, and that message is delivered to all members of the group.
Forward to Group Pager	n/a	Forward to Group Pager sends a page to the group pager when no members of the original group can take the call. The group's Pager field must be specified to forward to the group pager. Otherwise, this field is not enabled.
Forward to Another Badge, Group, or Address Book Entry	n/a	Forward to Another Badge, Group, or Address Book Entry transfers the call to a particular badge user, group, or address book entry when no members of the original group can take the call. To choose this option, click Select to open a dialog box that lists all the choices in the system. Select a badge user, group, or address book entry and click Finish. When you forward to a group, the forwarding settings of individual group members are ignored.
Forward to Another Number	70	Forward to Another Number transfers the unanswered call to the number that you enter. This feature requires the telephony integration option.
Forward to an Off-network Group Member	n/a	Forward to an Off-network Group Member enables on-call group members to receive calls when they are off-network.

Field	Maximum Length	Description
Forward When	n/a	Specify either of the following: • All forwards every call that comes in to the group, without notifying group members. • Unanswered forwards only calls that are not answered by any member of the group. If you provide a value other than All or Unanswered in the data-loading template, an error will occur when you try to import the file.

Group Permissions

The Permissions page of the Add/Edit Group dialog box lets you control the ability of users to issue certain commands or perform specific operations.

Table 20: Group permissions fields

Field	Description
Group of users permitted to manage this group	To let members of an existing group manage the group you are creating or editing, click the Select button under Group of users permitted to manage this group to display the Select Group dialog box. Choose a group that has management privileges, and then click Finish. Members of a group that has management privileges can add members to and remove members from the group you are creating. For example, you may want to assign the members of Head Cashiers management privileges for Cashiers so they can add members to the Cashiers group. If you edit the built-in Everyone group, the Select button does not appear. You cannot specify a group to manage the Everyone group — Vocera maintains membership in the Everyone group automatically. To clear this field, click the C button next to the value.
Group of users permitted to add themselves to this group	To let members of a group add themselves to the group you are creating or editing, click the Select button under Group of users permitted to add themselves to this group to display the Select User or Group dialog box. Choose a group that has this permission, and then click Finish. For example, you may want to assign members of the Nurses group the permission to add themselves to a group called On Duty. If you edit the built-in Everyone group, the Select button does not appear. You cannot allow members of another group to add themselves to the Everyone group — Vocera maintains membership in the Everyone group automatically. To clear this field, click the C button next to the value.
Group of users permitted to manage group's devices	To let members of an existing group manage the Vocera devices owned by this group, click the Select button under Group of users permitted to manage group's devices to display the Select Group dialog box. Choose a group, and then click Finish. The group you select requires no special privileges. Members of the group can modify information for the devices the managed group owns. Group device managers can edit basic device information, but they cannot view or modify devices owned by groups they do not manage. For more information, see **Group Device Managers** on page 68. If you edit the built-in Everyone group, the Select button does not appear. You cannot specify a group to manage devices for the Everyone group. To clear this field, click the C button next to the value.
Member permissions	Specify permissions for the group by selecting an item in the list of Member Permissions and clicking one of the following buttons: • Click Grant to grant members in the group the authority to perform the selected action. A green icon appears next to the action. • Click Revoke to ensure that members in this group do not have the authority to perform the selected action, even if membership in another group has granted it. A red icon appears next to the action. • Click Clear to reset the permission for the selected action. The icon next to the action is removed. You can use the Ctrl or Shift keys while you click items in the list to select more than one at the same time.

The Group Conference

The Conference page of the Add/Edit Group dialog box lets you maintain the list of users who are in the conference with the same name as the group.

You cannot actually add a *group* to a conference, but you can add all its *members* to the conference. Specifically, if you select a group when you populate a conference, you add only those users who are group members *at that time* to the conference—the conference *does not* reflect the dynamic membership of the group.

For example, if Lola Pergasz and Graden Close are members of the Clerks group at the time you add it to the Sales conference, they are both placed in the Sales conference. However, if Graden later leaves the Clerks group, he is not automatically removed from the Sales conference. Similarly, if Mariah Delaney later joins the Clerks group, she is not automatically added to the Sales conference.

Adding group members to a conference is only a convenience. Vocera distinguishes between group members and conference users because an individual can be a member of *multiple groups*, but that same person can be in only *one conference* at any time.

To specify the conference users:

1. Click Groups in the navigation bar.
2. Click Add Name on the Conference page, select the users from the list that appears, and then click Finish.

   > **Note:** If you add the members of a group to the conference, the Conference Users list displays the names of all the users who are members of the group at that time, not the name of the group.

   The Conference page displays the names you selected in the Conference Users list.
3. To remove users from the list, select their names and click Delete Name.
4. Do any of the following:
   - Click Save to create the group, close the Add New Group dialog box, and return to the Add, Edit, and Delete Groups page.
   - Click Save & Continue to create the group and leave the Add New Group dialog box open to create another group.
   - Click another tab in the Add New Group dialog box to enter additional group information.

Deleting Groups

When you delete a group from the system, the data related to the group is permanently removed and the name is no longer recognized. You can delete a group at any time.

To ensure that no call activity is interrupted, however, the deletion takes effect as soon as the system has no calls or Genie sessions in progress.

To delete groups:

1. Click Groups in the navigation bar.
2. Select one or more groups to delete.

   To select two or more adjacent rows on the Groups tab, click the first row, then hold down SHIFT while you click the last row to select.

   To select two or more nonadjacent rows on the Groups tab, click the first row, then hold down CTRL while you click other rows to select.

   To search for the group name instead, begin typing it in the Search field. As you type, a drop-down list appears with up to 10 matching names. Select one, or click Search to go to the first match.
3. Click Delete Group.

   A message asks you to confirm the deletion.

4. Click OK.

Maintaining Department Groups

The Departments page lets you maintain all your department and subdepartment groups together.

The Departments screen lets you see a list of all the groups you have designated as departments and subdepartments, add existing groups to the department list, and remove groups from the department list.

You can also specify whether an individual group is a department or subdepartment when you add it or edit it, as described in **Adding or Editing a Group** on page 74.

Note: You do not use the Departments page to add or delete a group itself, or add members to a group. You use the Departments page to make an existing group a department or subdepartment or to remove it from the list of groups that are used as departments.

Figure 7: Departments page

To add departments:

1. Click Departments in the navigation bar to display the Departments page.
   The Department Groups box lists any groups you are already using as departments or subdepartments.
2. Click Add Department to display the Select Group dialog box.
3. Choose groups from the list that appears, and then click Finish.
   The groups appear in the Department Groups list.

To choose subdepartments:

1. Click Departments in the navigation bar to display the Departments page.
   The Department Groups box lists any groups you are already using as departments or subdepartments.
2. Choose a group in the Department Groups list, and then click Choose Subdepartments to display the Choose Subdepartments dialog box.
3. In the Subgroups list, select any groups that you want to make subdepartments, and then click >> to move them into the Subdepartments list.

   Note: You cannot use the Departments page to add members to a group. To add members to a group, edit the group on the Groups page.

4. In the Subdepartments list, select any groups that you want to make subgroups, and then click << to move them into the Subgroups list.

5. Click Save to save the settings and close the Choose Subdepartments dialog box.

To remove a department or subdepartment:

1. Click Departments in the navigation bar to display the Departments page.

   The Department Groups box lists any groups you are already using as departments or subdepartments.

2. Choose a department in the Department Groups list, and then click Delete.

3. You are prompted whether it is OK to remove the department or subdepartment. Click OK.

   The group is removed from the Department Groups list. However, the groups is NOT removed from the Vocera system. Instead, its Group Type has been changed from Department or Subdepartment to Ordinary, making it an ordinary group.

Working with Permissions

Permissions control the ability of users to issue certain commands or to perform specific operations.

For example, you can allow certain users to make toll calls, but prevent other users from doing so.

For ease of use and flexibility, you assign Vocera permissions to groups of users—you do not assign permissions to individuals, and you do not override permissions on an individual basis. When you add or edit a group, the Permissions page in the Groups screen of the Administration Console lets you manage the permissions that you grant or deny to the members of that group.

Because you specify permissions at the group level, you can associate a permission with a role, rather than an individual user. For example, suppose you want the floor manager who is working at any given time to have the Record Name Prompts for Another User permission. You can create a group called Manager On Duty and grant the group that permission. Then the current floor manager will always have the Record Name Prompts for Another User permission, regardless of who that user is.

For a complete description of each permission, see Permissions Reference on page 234.

Accumulating Permissions

The complete set of permissions available to any single user is the total list of permissions granted to all the groups of which he or she is a member.

For example, suppose the Staff group grants the Call Internal Numbers and the Call Toll-Free Numbers permissions and the Manager group grants the Call Toll Numbers permission. If a user is a member of both Staff and Manager, that user has the Call Internal Numbers, Call Toll-Free Numbers, and Call Toll Numbers permissions.

Table 21: Permissions for Staff and Manager groups

Permission	Staff	Manager	Staff & Manager
Call Internal Numbers	Yes		Yes
Call Toll-Free Numbers	Yes		Yes
Call Toll Numbers		Yes	Yes

Changes to permissions take effect immediately. For example, if you edit the Manager group to grant the Have VIP Status permission, everyone in the Manager group immediately gains that permission. You do not need to apply the permission or require users to log in again.

Default Permissions

Because the **Everyone Everywhere** group includes every user on the system, this group establishes the default permissions for all your Vocera users.

For example, suppose you want to grant every user across all sites certain basic permissions, such as Call Internal Numbers and Call Toll-Free Numbers. You can specify these permissions in the **Everyone Everywhere** group, then grant additional permissions by providing membership in additional groups.

Similarly, an **Everyone** group establishes a set of default permissions for the specific site it is associated with. For example, suppose you want to grant all sites the Call Internal Numbers and Call Toll-Free Numbers permissions, but grant only the North Beach site the Call Toll Numbers permission. Grant **Everyone Everywhere** the Call Internal Numbers and Call Toll-Free Numbers permissions, then grant the North Beach **Everyone** group the Call Toll Numbers permission.

If your Vocera deployment does not implement multiple sites, you can ignore the **Everyone Everywhere** group and set default permissions in the Global **Everyone** group.

Permissions for the "Everyone" Group

When you first install or upgrade Vocera, you have only a single **Everyone** group—the one associated with the Global site.

The permissions you assign to this Global **Everyone** group act as a template and provide an initial set of permissions for successive site-specific **Everyone** groups.

You can change the initial set of permissions that new **Everyone** groups acquire to enforce different policies at different sites. The permissions of the Global **Everyone** group act only as a convenient template, providing an initial set of permissions for the site-specific **Everyone** groups that follow.

Do not confuse the permissions template provided by the Global **Everyone** group with the permissions users inherit from the **Everyone** group for their site. Users do not inherit permissions from the Global **Everyone** group; they inherit permissions from their site-specific **Everyone** groups.

See About the Built-In "Everyone" Group on page 69 for more information.

Revoking Permissions

The **Revoke** button cancels a permission that a user would otherwise have by virtue of membership in another group.

You can revoke a permission to ensure that a group of users does not have a specific permission, even if membership in another group grants that permission.

For example, if your site issues courtesy badges to visitors, you can use **Revoke** to make sure that visitors do not have certain Vocera permissions. Suppose the Everyone group grants the Call Toll Numbers permission. Because Vocera automatically adds all users to the Everyone group, visitors are also granted that permission automatically.

To disable this permission for visitors, you can create the Guest group, then revoke the permission for Call Toll Numbers in it. When you add all visitors with courtesy badges to the Guest group, they will have all the permissions granted by membership in Everybody except Call Toll Numbers, which is revoked by membership in Guest.

Permissions for Administrators

Vocera provides a special permission for system administrators that automatically grants most permissions and overrides any revoked permission.

In addition, Vocera provides a range of permissions for tiered administrators, granting different levels of access to administrative features. See System and Tiered Administrators on page 25.

Using the Permission Browser

The Permission Browser is a tool that allows system administrators to browse a user's or group's hierarchy of group memberships to identify the status of revoked or granted permissions.

The Permission Browser can help you quickly identify how a user has been granted or revoked a particular permission by stepping through the groups to which a user belongs. You can also use the Permission Browser to modify the permissions of groups, or compare permissions of one user or group with another.

If the Vocera Voice Server has enabled SSL, you may need to update Internet Explorer security settings before you can use the Permission Browser. See **Updating Browser Security Settings for SSL Access** on page 29.

> **Note:** The Permission Browser is available only to users with system admnistration privileges. If you log into the Administration Console as a user without system administration privileges, the Permission Browser tab is not visible.

To browse the permissions for a user or group:

1. Log into the Administration Console as a user with system administration privileges. See **Permissions for Administrators** on page 84 for details.
2. Click Groups in the navigation bar.
3. Select the Permission Browser tab to display the Permission Browser page.
4. Under the Membership Hierarchy Browser list, click Add Name. The Select User Or Group dialog box appears.
5. Select a user or group, and then click Finish.

   > **Note:** You can search for the name of a user or group. You can also filter the list by site.

6. Navigate the group hierarchy.
   1. Click ▶ to open a group hierarchy.
   2. Click ▼ to close a group hierarchy.

   > **Tip:** The Membership Hierarchy Browser list displays the group hierarchy in *reverse order*. In other words, parent groups are shown below their children.

7. As you click groups to step through the hierarchy, the Permissions List is updated to show the permissions for the selected group.
8. To modify a permission for a group:
   1. Select a permission in the Permissions List.
   2. Click Grant to grant the permission or Revoke to revoke it. Click Clear to remove the granted or revoked status.
   3. Click Save to save the change.

   > **Note:** Although the Permission Browser allows you to modify a group's permissions, it does not let you change its membership. If you would rather change the group's membership, see **Adding or Editing a Group** on page 74.

Parts of the Permission Browser Screen

On the right side, the Permissions List shows the resulting permissions for the selected user or group.

The Permission Browser page has two sections:

- On the left side, the Membership Hierarchy Browser lists the hierarchy of groups for users or groups that you add to the list by clicking Add Name.

  The Membership Hierarchy Browser uses the following icons to identify users and groups:

- 🧑 = User
- 👥 = Group
- If a group is selected in the Membership Hierarchy Browser, the permissions list on the right also shows permissions that have been granted or revoked for that group.
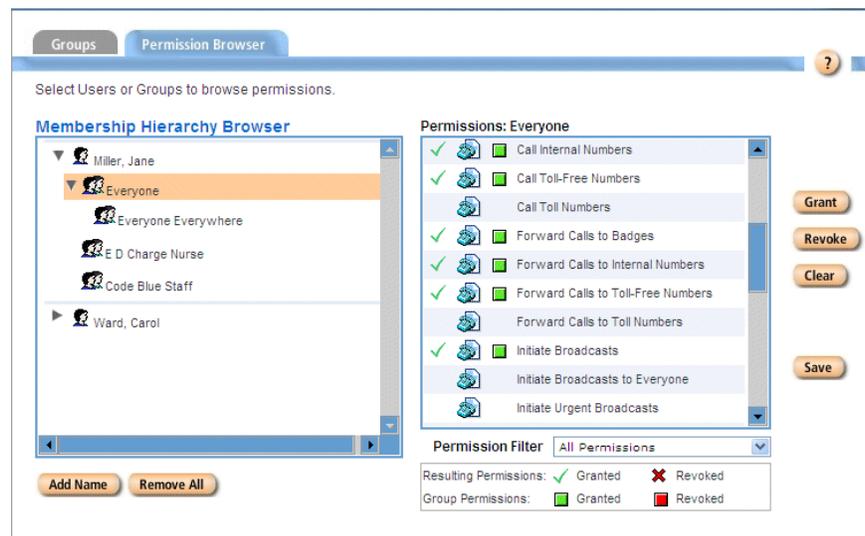
Figure 8: Permission Browser page

Permission Browser Buttons

The following table describes the different buttons available on the Permission Browser page:

Table 22: Permission Browser buttons

Button	Description
Add Name	Adds a user to the Membership Hierarchy Browser list. When you click Add Name, the Select User Or Group dialog box appears.
Remove Name	Removes the selected user or group from the Membership Hierarchy Browser list. The Remove Name button is shown only when a top-level user or group is selected in the Membership Hierarchy Browser list.
Remove All	Removes all users and groups from the Membership Hierarchy Browser list.
Grant	Grants the permission to the selected group. If a user is currently selected in the Membership Hierarchy Browser, the Grant button is not shown.
Revoke	Revokes the permission for the selected group. If a user is currently selected in the Membership Hierarchy Browser, the Revoke button is not shown.
Clear	Clears the granted or revoked status of the permission for the selected group. If a user is currently selected in the Membership Hierarchy Browser, the Clear button is not shown.
Save	Saves the granted or revoked status of the permission for the selected group. If a user is currently selected in the Membership Hierarchy Browser, the Save button is not shown.

Permission Filter

You can filter the Permissions List by using the Permission Filter below the list. Select whether to show All Permissions or only Granted/Revoked Permissions.

Permissions List Icons

Learn the available controls on the Permission Browser.

The Permissions List on the right side of the Permission Browser has the following fields:

Table 23: Permissions List fields

Field	Description
Resulting Permission	Displays one of the following icons identifying the resulting permission from the selected group as well as permissions inherited from parent groups (if any). • ✓ = Granted • ✖ = Revoked
Permission Category	Displays one of the following icons identifying the permission category: • 🔑 = System Administrator permission • = Tiered Administrator permission • = Call permission • = Security permission • = Special permission
Group Permission	Whether the permission is explicitly granted or revoked for the group. • ■ (green) = Granted • ■ (red) = Revoked
Permission Name	The name of the permission.

The resulting permission can be different from the group permission if a permission is inherited from a parent group. For example, in the following figure the resulting permission of Call Toll Numbers is revoked ✖ for the EMT Nurse group even though the permission is explicitly granted ■ for the group. This means that the permission must have been revoked in a parent group.
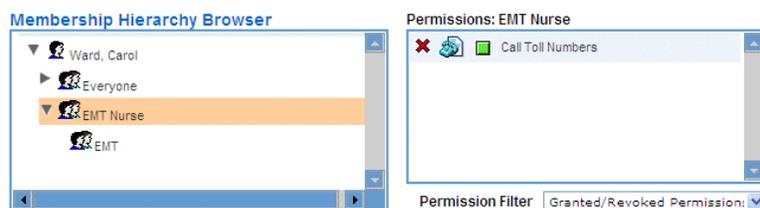
Figure 9: Resulting permission different from group permission

The following figure shows the parent group EMT selected. The Call Toll Numbers permission has been revoked in this group. The EMT Nurse group inherited the revoked Call Toll Numbers permission from the EMT group.
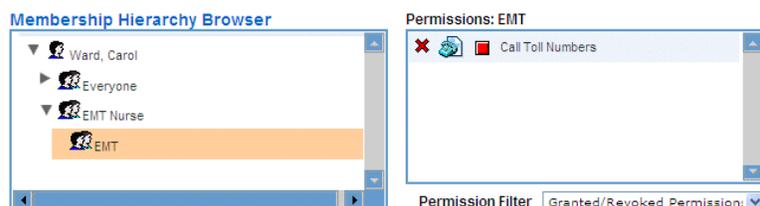
Figure 10: Call Toll Numbers permission is revoked

Comparing Permissions of Different Users or Groups

You can click Add Name to add multiple users or groups to the Permission Browser.

Once the users or groups have been added to the Membership Hierarchy Browser, you can step through the hierarchy to compare the permissions and group membership for each.

Tip: During an Administration Console session, the Permission Browser maintains the users or groups you have added. You can leave the Permission Browser temporarily to do other things in the Administration Console, and then return later to continue browsing permissions.

Working with Favor Frequently Called for Users and Departments

The Favor Frequently Called feature for departments and users takes advantage of users and departmental calling patterns to improve speech recognition.

When the Favor Frequently Called feature for users and departments is enabled, the Vocera Voice Server accumulates data about the frequency of calls made to a circle of users, or from users in one department to users in another (or the same) department.

When a call is made, the server uses this data to weight user names and departments in the speech recognition grammars, favoring members of more frequently called users or departments. This weighting improves overall speech recognition considerably.

For example, the Genie may have trouble distinguishing between the phonetically similar commands, "Call Phil Rains" and "Call Phil Ray". If "Phil Rains" is a frequently called user and the Call command is issued for him, the Genie gives preference to "Phil Rains". Similarly, if you have the Favor Frequently Called feature for departments enabled, the Genie weighs a frequently called user belonging to a particular department over an individual in a different department name. For example, if Juanita Gonzalez in Cardiology is frequently called, she will be weighted over Juanita Gonzalez in Emergency.

> **Note:** The Favor Frequently Called feature for users and departments **cannot** be enable at the same time. You must choose this feature for either users or departments and never for both. For assistance determining which feature is better for your environment, contact Vocera Customer support.

How to Enable Favor Frequently Called for Departments

The Frequently Called Feature for Departments feature takes several weeks of calling statistics to determine reliable calling patterns for departments.

You can disable or re-enable the Favor Frequently Called feature for departments on the System > Preferences page of the Administration Console.

The Frequently Called feature for departments works best when all the users, who you want in the frequently called department, are assigned to a department. However, users who are not assigned to a department (such as temporary visitors to a site), can use a special grammar file to aid in succenful implementation.

To enable the Frequently Called feature for departments:

1. In the Administration Console, choose System > Preferences.
2. In the Favor Frequently Called box, select Enable for Departments.
3. Click Save Changes.

Collecting Call Statistics for Frequently Called Departments

For each department group, the Vocera Voice Server collects statistics for the top 10 frequently called departments made by people in the department, and it recalculates the probabilities for calling patterns incrementally after each 50 calls.

Calling patterns do not take effect until after the first week's statistics have been collected. The system preserves calling statistics for the last five weeks and discards earlier data.

Viewing Call Statistics for Frequently Called Departments

After you set up department groups and subdepartment groups, you may want to view calling statistics for a specific department.

You can see which departments that people within a selected department typically call, including their own department.

If you believe the current calling statistics for a site or a department group do not accurately reflect calling patterns, you can clear the data and begin collecting data all over again.

To view calling statistics for Frequently Called Departments:

1. Click Departments in the navigation bar to display the Departments page..
2. Click the Dept Call Frequency tab.
3. In the Select Site list, select a site or use the default Global site.
4. In the Select Department list, select a department group.

To clear calling statistics for Frequently Called Departments:

1. Click Departments in the navigation bar to display the Departments page..
2. Click the Dept Call Frequency tab.
3. In the Select Site list, select a site or use the default Global site.
4. In the Clear Calling History For box, click one of the following buttons:
   - Selected Site – clears calling history for the selected site.
   - Selected Department – clears calling history for the selected department.
   .

Best Practices for Frequently Called Departments

To take full advantage of the Frequently Called Departments feature to improve overall speech recognition for the Vocera system, Vocera recommends the best practices listed in this topic.

1. If your Vocera system is very large, you may need to do some performance tuning to optimize your system. A large Vocera system typically has more than 2,500 users across multiple sites and a spoken name count (which includes user names, group names, alternate spoken names, and department names) equal to or greater than 90,000. See **Performance Tuning for Large Customers** in the *Vocera Infrastructure Planning Guide*.

2. Make sure Frequently Called Departments options are enabled on the **System > Preferences** page of the Administration Console. See Setting System Preferences on page 109 for complete information.

3. Use the Departments page of the Administration Console to define your department and subdepartment groups. See Maintaining Department Groups on page 81 for complete information.

4. Make sure all Vocera users are assigned to a department.Also, avoid nesting department groups.

   Users who are members of a department will benefit from speech recognition improvements due to the Frequently Called Departments feature. All users who are not assigned to a department use a special speech recognition grammar file that is assigned a 5% probability.

5. Allow calling statistics to be collected for several weeks to determine reliable calling patterns for departments. Before calling patterns take effect, uniform probabilities are applied to departments. See Collecting Call Statistics for Frequently Called Departments on page 90 for complete information.

6. In the Administration Console, you can view calling statistics for Frequently Called Departments on the Dept Call Frequency tab of the Departments page. If department and subdepartment groups have experienced significant changes in membership due to restructuring of your Vocera database, you may want to clear the calling statistics for a selected site or department. See Viewing Calling Statistics for Frequently Called or department. See Viewing Call Statistics for Frequently Called Departments on page 90 for complete information.

7. To assess speech recognition for departments, use the Vocera Report Server to schedule several diagnostic reports, including Recognition Results by Department and Recognition Results by User. For more information, see the *Vocera Report Server Guide*.

How to Enable Favor Frequently Called for Users

The Favor Frequently Called feature for users function is based on the premise that users call the same set of users on a regular basis.

The list of users in the Favor Frequently Called feature is used to prefer the frequently called members in the voice recognition result. Buddies are automatically added to the frequently called list and stored in the same database as other frequently called users.

You can enable or disable the Favor Frequently Called feature for users globally and for individual users in the Administration Console:

- System > Preferences page of the Administration Console
- User > Edit User > Speech Rec page of the Administration Console

In addition, you can override defaults and other settings for the Favor Frequently Called feature for users in Default > Advanced Speech Recognition. For more information, see Choosing Advanced Speech Settings on page 123.

To enable Favor Frequently Called Users:

1. In the Administration Console, choose System > Preferences.

2. In the Favor Frequently Called box, select Enable for Users.

3. Click Save Changes. The default is now set for all users to have Frequently Called Users enabled.

Next Steps: To enable and disable this feature for individual users, go to Users > Edit User > Speech Rec page.

> **Note:** Favor Frequently Called feature for users does not have statistics available at this time.

Status Monitor and Address Book

This section describes how to use the Status Monitor and Address Book, and how to configure email integration.

Status Monitor

The Status Monitor screen provides pages that display information about badge users, groups, and devices that have been assigned to groups.

For example, you can find out which users and which members of a group are currently logged in, and you can see the devices currently on the network.

Badge Status Monitor

Learn the information you can monitor for logged-in users.

The Badge Status Monitor page displays the following information about logged-in users and their badges:

Table 24: Badge Status Monitor fields

Field	Description
Full Name	Shows the names of all users who are currently logged in.
IP Address	Shows the network address of the badge. If the network address is assigned dynamically through the DHCP server, the IP address can change as the user moves between access points.
Call Status	Shows the `Call Status` if the user is active in a call, or `Inactive` if the badge is idle. The Call Status shows `Genie` if the user is doing any activity that requires the Genie, such as giving a command, getting messages, or recording a name or greeting. It also reveals the following forwarding status: • `Forwarding Offline`: Calls are being forwarded for an offline user. • `Forwarding Unanswered`: Calls are being forwarded when the user does not answer. • `Forwarding All`: All calls are being forwarded for the user.
DND/Hold	Shows `DND` if the user has put the badge in Do Not Disturb mode, or `Hold` if the user has placed a call on hold. Otherwise, this field is blank.
Location	Shows the name of the location of the access point to which the user is currently connected. If a location name was not assigned, the field shows the access point's MAC address.
Current Site	Shows the name of the physical site where the user is currently logged in.

Use the Badge Status Monitor page to perform the following tasks:

• To update the display immediately, click Refresh or click a column heading to change the sorting method. The default setting for the display shows user names sorted alphabetically, last name first.
• To sort users by IP Address, Call Status, DND/Hold status, Location, or Current Site, click the corresponding column heading.
• To return to alphabetical sorting, click the Full Name column heading.
• To list the users logged in at a specific site, choose a site from the Site Filter list.

- To search for a specific user, type a last name or part of a last name in the Search field, then click Search.

- To upload Vocera badge logs, select a badge, and then click Upload Logs.

  When you upload badge logs, the files are assembled into a single `.tar.gz` file in the `\vocera\logs\BadgeLogCollector\uploads` directory on the Vocera Voice Server. The format of the filename is `DATETIME-USERNAME-BADGEMAC-udd.tar.gz`.

  > **Note:** You cannot upload logs for Vocera smartphones from the Administration Console.

The Vocera Voice Server updates the Badge Status Monitor according to the number of seconds you set as the Refresh Interval. To specify a different time between automatic updates, type a value of 20 or greater in the Refresh Interval field and press Enter.

To display the Badge Status Monitor:

1. Click Status Monitor in the navigation bar.
2. Click the Badge Status tab.

Group Status Monitor

Learn the information you can monitor for logged-in members of a group.

The Group Status Monitor page displays the following information about logged-in members of a group:

Table 25: Group Status Monitor fields

Field	Description
Groups	Displays the name of every group, in alphabetical order. Users with System Administrator permission can see all groups in the Group Status Monitor. Group managers can see only groups they are permitted to manage. Users with the View Users and Groups permission can see all groups by checking the View All Groups box at the bottom left of the page.
Active Users	Displays the total number of *immediate* group members who are logged in. Users who are members of a *nested group* are not included in this total. Nested groups appear alphabetically within the list; they are not displayed hierarchically under parent groups.
Site	Shows the name of the physical site the group is associated with.

To display a list of the logged-in members of a group, expand the group by clicking the triangle at the left of the group's name and icon.

After you expand a group, the Group Status Monitor displays columns of information for each of the group members. This is the same information that appears in the Badge Status Monitor, except it is sorted by group. See **Badge Status Monitor** on page 94 for a description of these columns.

You can display the members of one group at a time only. For example, you can display a list of members in the Doctors group, or you can display a list for the Nurses group, but you cannot display both member lists at the same time.

You can also use the Group Status Monitor page to perform the following tasks:

- To update the display immediately, click Refresh. Vocera closes any open group in the list and refreshes the information for all groups.

- To list only the groups at a specific site, choose a site from the Site Filter list.

- To locate a specific group, type a name or part of a name in the Search field, select it from the list, then click Search.

- If you have the View Users and Groups permission, you can view all groups in the selected site by checking the View All Groups box at the bottom left. Otherwise, the View All Groups box is diabled, and you can view only groups that you manage. System administrators always view all groups, so the View All Groups checkbox is disabled for them.

The Vocera Voice Server updates the Group Status Monitor according to the number of seconds you set as the Refresh Interval. To specify a different time between automatic updates, type a value of 20 or greater in the Refresh Interval field and press Enter.

To display the Group Status Monitor:

1. Click Status Monitor in the navigation bar.
2. Click the Group Status tab.

Device Status Monitor

Learn the information you can monitor for devices that have been assigned to a group.

The Device Status Monitor page displays the following information about devices that have been assigned to a group:

Table 26: Device Status Monitor fields

Field	Description
Device Groups	Displays the name of every group that manages devices, in alphabetical order. If you have Perform System Administration or Perform System Device Management permissions, you can monitor devices for all groups. If you are a group device manager, you can monitor devices only for groups you are permitted to manage.
Total Devices	Displays the total number of devices owned by the group. Devices that are owned by a nested group are not included in this total. Nested groups appear alphabetically within the list; they are not displayed hierarchically under parent groups.
Active Devices	Displays the total number of devices owned by this group that are pinging the server. The devices do not need to be logged into the system, but they do need to be assigned to a group.
Site	Shows the name of the physical site the group is associated with.

> **Important:** Devices that have not been assigned to a group yet are not listed on the Device Status Monitor page, even though such unassigned devices can still be used to log into the system and appear on the Badge Status Monitor page.

To display a list of devices owned by a group, expand the group by clicking the triangle at the left of the group's name and icon.

After you expand a group, the Device Status Monitor displays columns of information for each active device. This is similar to the information that appears in the Badge Status Monitor, except it is sorted by group and it includes the serial number and device label. See **Badge Status Monitor** on page 94.

If a user is not logged into a device and it is currently in a battery charger, the Full Name field for that device displays "Not logged in" and a lightning bolt icon appears to the right of the badge icon.

You can display the devices of one group at a time only. For example, you can display a list of devices in the Doctors group, or you can display a list for the Nurses group, but you cannot display devices for both groups at the same time.

You can also use the Device Status Monitor page to perform the following tasks:

- To update the display immediately, click Refresh. Vocera closes any open group in the list and refreshes the information for all groups.

- To list only the groups at a specific site, choose a site from the Site Filter list.
- To locate a specific group, type a name or part of a name in the Search field, select it from the list, then click Search.

Note: You cannot search for devices that are owned by a particular group.

The Vocera Voice Server updates the Device Status Monitor according to the number of seconds you set as the Refresh Interval. To specify a different time between automatic updates, type a value of 20 or greater in the Refresh Interval field and press Enter.

To display the Device Status Monitor:

1. Click Status Monitor in the navigation bar.
2. Click the Device Status tab.

Using the Address Book

The address book is a convenient way for badge users to contact places and people who are not badge users.

For example, if people in your organization frequently need to contact local businesses, you can enter the business names and nicknames in the address book. Then, getting a price quotation from Northwestern Hardware can be as simple as using the badge to say "Call Northwestern."

The distinction between whether a name is maintained in the address book or in the directory is usually transparent to badge users. In either situation, badge users can simply say "Call Michelle Spangler" to reach the person to whom they want to speak.

Address book entries are available to anyone who has access to the Vocera system; they do not require permissions. For example, a user does not need the Call Toll Numbers permission to call an address book entry that you define with a toll phone number.

Incoming phone calls from outside the Vocera system that reach the Genie prompt ("Please say the name of the group or person you want to reach") can ask for an address book entry also.

Using Voice Commands with Address Book Entries

Learn the voice commands you can use when accessing a device other then the Vocera Badge.

Badge users can issue the following voice commands with address book entries:

- Call
- Conference
- Forward
- Invite
- Learn
- Send Email
- Send a Page
- Transfer
- Unlearn

Recording a Name for an Address Book Entry

By recording name prompts yourself, the Genie can use them to provide more natural sounding speech and to avoid mispronunciations.

The Genie speaks the name of address book entries when interacting with users. For example, the Genie speaks the name of a person or place in the address book when confirming a call that a user makes to an address book entry.

The Genie can synthesize name prompts for an address book entry.

1. Log in with a badge as a user with system administration privileges. See Permissions for Administrators on page 84 for details.

2. Press the Call button, wait for the Genie to answer, and then say, "Record a name for *person or place name.* " (For example, "Record a name for Poison Control.")

> **Note:** If multiple sites, users, groups, locations, and address book entries have the same name or alternate spoken name, you can record a name prompt for only one of them.

The Genie will prompt you to record the name.

The Address Book for the Global Site

If you have multiple sites and have enabled telephony for the Global site, you can use the Global address book to store contact information for people and places that users from all sites need to access.

> **Note:** If you have not enabled telephony for the Global site, you cannot make calls to Global address book entries.

The address book associated with the Global site is equally accessible to all users, regardless of the physical site they are working at. That is, if an entry is in the global address book, users at any site can access it by name only—they do not have to specify the site name.

For example, suppose all the sites in your organization frequently place orders from a wholesaler outside the company. Because the wholesaler is not within the Vocera system, you should place its contact information in an address book; in addition, because users at any site may need to call the wholesaler, its information belongs in the address book for the Global site.

In this situation, any user can call the wholesaler by saying "Call Spangler Supplies". If Spangler Supplies were associated with a site-specific address book such as San Jose, users outside San Jose would have to say, "Call Spangler Supplies in San Jose".

See **About the Global Site** on page 35.

Adding or Editing an Address Book Entry

When you add or edit an address book entry, you provide basic information to identify the entry, then you optionally provide speech recognition information.

> **Note:** When you need to add a large number of address book entries, you can save time by importing them directly from CSV files to the Vocera database. See **Importing Data from a CSV File** on page 162.

The Add/Edit Entry dialog box provides two pages where you can enter information: the Entry Information page and the Speech Recognition page.

To add or edit an address book entry:

1. Click Address Book in the navigation bar.
2. Click Add New Entry to add a new entry, or choose a name from the list and click Edit Entry to edit an existing site.
   The Add/Edit Entry dialog box appears.
   The Search for Entry option can help you find a name quickly. As you type a name, Search for Entry finds the closest match in the list.
3. Enter basic information in the Entry Information page.
   See **Basic Entry Info** on page 100.
4. (Optional) Enter speech recognition information in the Speech Recognition page.
   See **Speech Recognition** on page 101.
5. Save your address book entry in either of the following ways:
   - Click Save to save the entry and return to the Add, Edit, and Delete Entries page.

- Click Save & Continue to save the entry and begin entering a new address book entry.

Basic Entry Info

Use the Entry Information page (or the corresponding fields in the data-loading template) to provide basic information about a specified address book entry. The Entry Information page includes the following fields:

Table 27: Address book information fields

Field	Maximum Length	Description
Entry Type	n/a	Use the Entry Type radio buttons to identify the type of entry you are adding to the address book: • Choose Person to specify that the contact information you are providing is for an individual. • Choose Place to specify that the contact information you are providing is for a place. **Note:** This field does not appear in the Address Book data-loading template. In the template, you implicitly specify the entry type as a person by providing a value in the First Name column or as a place by leaving the First Name column blank.
First Name, Last Name, Name	50	Provide a name for the address book entry as follows: • If you are entering contact information for a person, use the First Name and Last Name fields to specify the full name of the individual. • If you are entering contact information for a place, use the Name field in the Add/Edit dialog box (called Last Name or Place Name in the Address Book data-loading template) to specify the name of the organization or place. The name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed. By default, the speech recognition system uses the name you enter to recognize address book entries. If users refer to an address book entry by something other than the name you enter here, provide an Alternate Spoken Name in the Speech Recognition tab.
Phone	75	Optionally provide a phone number for the person or place in the Phone field.
Pager	75	Optionally provide a pager number for the person or place in the Pager field. If you enter a value for this field, any user can issue the "Send a page" voice command to send a numeric page to this address book entry; when the recipient returns the call, it is connected directly to the user's badge. To identify this pager as a Vocera Messaging Platform pager number, prefix the number with a "w".
Email Address	40	Optionally enter an Email Address to allow users to send voice messages as an email attachment. **Note:** You must also configure the settings on the Email page of the Administration Console to enable this feature.
Site	50	Use the Site field to specify the home site for the address book. In the Add/Edit Entry dialog box, click the Select button to open the Select Site dialog box, then choose a name from the list and click Finish. • If your organization has multiple sites connected to the same Vocera Voice Server, choose the home site where users need to access this address book entry. If the entire organization uses this entry, choose Global. • If your organization does not have multiple sites, accept the default Global setting. When working in the data-loading template, leave this field blank to accept Global.

Speech Recognition

Use the Speech Recognition page (or the corresponding fields in the data-loading template) to provide alternate spoken names, phonetic spellings, or additional identifying information so the speech recognition software can recognize variations of a name. The Speech Recognition page includes the following fields:

Table 28: Speech recognition fields

Field	Maximum Length	Description
Alternate Spoken Names	50	Optionally use the Alternate Spoken Names fields to enter variations of the name in your address book. The name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed. • If users refer to a person or place in various ways, enter each variation in a different field. For example, enter `Bob Jones` and `Rob Jones` in addition to `Robert Jones`. Similarly, enter a nickname that the person or place is known by, such as `Skip Jones`. • If people use an acronym or initials to refer to an address book entry, provide them as a series of letters separated by spaces. For example, if users refer to Easton Medical Clinic as EMH, enter `E M H`. Similarly, enter `A C Hoyle` for A.C. Hoyle. • If a name has an unusual or confusing pronunciation, enter a name that is spelled as it is pronounced. For example, if the system does not recognize the name *Jodie Dougherty*, you could enter `Jodie Dockerty`. • If users refer to a person by his or her title, provide the full spelling of the title. For example, enter `Father Brown` instead of `Fr. Brown`.
Identifying Phrase	100	Optionally use the Identifying Phrase field to enter a description that distinguishes a person or place from another whose name is spelled the same. For example, if there are two Mary Hills on the system, but one is on the third floor and the other is on the first floor, you might enter `Mary Hill in the Main Cafeteria` as the Identifying Phrase for one user and `Mary Hill in the North Wing Cafeteria` for the other. As a result, when callers ask for Mary Hill, the Genie prompts them, "Do you mean Mary Hill in the Main Cafeteria?" If the caller says "no," the Genie then prompts, "Do you mean Mary Hill in the North Wing Cafeteria?"

Deleting Address Book Entries

When you delete an address book entry from the system, the data related to the entry is permanently removed and the name is no longer recognized.

You can delete an entry at any time. To ensure that no call activity is interrupted, however, the deletion takes effect as soon as the system has no calls or Genie sessions in progress.

To delete an address book entry:

1. Click Address Book in the navigation bar.
   The Add, Edit, and Delete Entries page appears.
2. Select one or more entries to delete.
   To select two or more adjacent rows on the Address Book tab, click the first row, then hold down SHIFT while you click the last row to select.
   To select two or more nonadjacent rows on the Address Book tab, click the first row, then hold down CTRL while you click other rows to select.

To search for the address book entry instead, begin typing it in the Search field. As you type, a drop-down list appears with up to 10 matching names. Select one, or click Search to go to the first match.

3. Click Delete Entry.

   Vocera asks you to confirm the deletion.

4. Click OK.

   Vocera removes the entry from the list and from the database.

Using Macros in Address Book Entries

Dialing macros enable you to create certain address book entries that are not possible otherwise. This section shows you how to use the address book to take advantage of these dialing macros.

It also provides examples of some other address book entries that you may want to implement. For information about dialing macros themselves, see **Special Dialing Macros** on page 231.

Calling Home

You can use the built-in dialing macros to create a single address book entry that any badge user can access to call home.

Vocera interprets the %H dialing macro in this example as the value you provided in the Home Phone field on the User Information page of the Add User dialog box. A user can also enter or change the Home Phone value in the User Console.

To create an address book entry for home:

1. Click Address Book in the navigation bar.

   The Add, Edit, and Delete Entries page appears.

2. Click the Add New Entry button.

   The Add New Entry dialog box appears.

3. Check Place in the Entry Type section.

4. Enter a name such as My House in the Name field. Make sure you use at least two words in the name for optimal speech recognition.

   Do not use the name "My Home" for this address book entry. Badge users can issue the command "Forward calls to my home phone" to forward calls when they are off-site. If users instead accidentally forward calls to the address book entry called "My Home" , other badge users who call them will experience unexpected results. Users should not forward calls to an address book entry that evaluates to the %H macro.

5. Enter %H in the Phone field.

6. Click Save to close the dialog box and save the entry.

When a user issues the voice command " Call My House, " Vocera automatically dials the specific user's home phone number.

Night-Bell Pickup

If your PBX uses a special code for after-hours pickup, you can create an address book entry for a place.

For example, call it **Night Bell** or **After Hours** — and enter the code in the Phone field. See **Entering Phone Numbers** on page 228 for information about the characters you can enter in the Phone field.

Forwarding Calls to a User's Pager

Calls to a group can be forwarded to the pager number for the group.

For information about editing a group, including the Pager field, see **Adding or Editing a Group** on page 74.

Vocera does not allow users to forward calls directly to a pager, because callers do not typically expect that behavior. Sending a page usually implies a sense of urgency or importance, and callers would be surprised if Vocera automatically forwarded a less critical call to a pager without opportunity for intervention.

However, some sites may have specific situations that warrant forwarding a user's calls to a pager. In this situation, you can set up an address book entry for the pager *itself,* and then forward the user's calls to this address book entry.

You cannot simply enter a phone number in the Pager field of an address book entry to achieve this effect. Supplying a value in the Pager field allows a user to issue the "Send a Page" voice command—it does not permit forwarding.

The rest of this section shows you how to use the built-in dialing macros to create an address book entry that permits indirect forwarding. Set the group properties to forward calls to this address book entry; when the recipient returns the call, it is connected directly to the original caller's badge.

> **Note:** Use the technique in this section only if or a user at your site needs to forward a call to a pager. To allow ordinary badge-to-pager interactions, enter a pager number directly in the user profile and in the address book entry.

To forward a user's calls to a pager:

1. Click the Address Book tab in the navigation bar.
   The Add, Edit, and Delete Entries page appears.
2. Click the Add New Entry button.
   The Add New Entry dialog box appears.
3. Check Place in the Entry Type section.
4. Enter a name such as **UserName**Pager in the Name field.
5. In the Phone field, enter the following values in this order:
   - Either a Q to indicate that the value in this field is a literal.
   - The access code that is needed for an outside line.
   - The long distance access code, if necessary.
   - The area code, if necessary.
   - The phone number of the pager.
   - A semicolon to separate the pager number from the numbers the pager will display.
     The semicolon causes Vocera to pause until the pager is ready to receive the numbers to display.
   - The Vocera hunt group dialing macro (%V).
   - The desk phone dialing macro (%D).
   - Any special characters, such as the # character, that the pager requires to end the sequence.

   For example, if the pager's number is (408) 555-1313, and it is a toll call, enter the following value in the Phone field (assuming the access code for an outside line is 9 and the access code for long distance is 1):

   Q 9, 1-(408) 555-1313 ; %V %D #

   > **Note:** Do not use a comma when you are connecting to a digital PBX. The comma character is not recognized by a digital PBX, and it may prevent a connection if it occurs after the access code.
6. Click Save to close the dialog box and save the entry.

When the user forwards a call to this address book entry, Vocera dials the pager number, pauses briefly, and then passes the pager the hunt group number and the desk extension of the user who called. The pager displays the hunt group number and the desk extension. If the caller does not have a desk extension, the pager displays only the hunt group number.

The pager's owner returns the call by dialing the hunt group number and then entering the badge user's desk extension at the hunt group Genie prompt. Vocera then automatically connects the return call to the user's badge.

Vocera interprets the %V dialing macro in this example as the value you provided in the Vocera Hunt Group Number field on the Basic Info page of the Telephony tab. Vocera interprets the %D dialing macro as the value you provided in the Desk Phone or Extension field on the User Information page of the Add User dialog box when you set up the user. A user can also enter or edit this value in the User Console.

System Settings, Defaults, Clusters, and Active Directory Authentication

This section describes how to set systemwide settings and defaults, configure and maintain clusters, and set up Active Directory authentication.

System Settings

The System screen of the Administration Console specifies default settings for the entire Vocera Communications System.

These settings are site-independent—they affect the entire Vocera system.

Displaying License Information

The License Info page of the System screen displays information about your Vocera Voice Server licenses. It also lets you specify a company name, a report server address, or refresh a new a temporary license.

The License Info page provides the following fields:

Table 29: License information fields

Field	Maximum Length	Description
Company Name	100	Specify the name of your company or organization. The value you enter in this field appears in reports and logs.
Report Server IP Address	50	If you are using a Vocera Report Server, specify its IP address. For security reasons, you must register the address of the Report Server with the Vocera Voice Server in this manner, or the Vocera Voice Server prevents the Report Server from downloading data. You must also enter the IP address of the Vocera Voice Server in the Report Console.
VAI Application IP Addresses (comma-separated list)	80	Optionally enter a comma-separated list of IP addresses to limit the list of computers which are allowed to establish VAI connections to the Vocera Voice Server. If you leave this field blank, a VAI application from any machine is allowed to connect to the Vocera Voice Server; however, applications still need to authenticate to access data on the Vocera Voice Server. A VAI application that is deployed directly on any node of a Vocera Voice Server cluster is automatically authorized to connect; you do not have to add it explicitly to the VAI Application IP Addresses field. **Note:** For Vocera Messaging Platform Integration, make sure your Vocera Messaging Platform server IP address(es) are in the VAI Application IP Addresses field. Enter the Vocera Messaging Platform server IP address first, before all other IP addresses that are running VAI applications.

Field	Maximum Length	Description
General License Info	n/a	Displays general information about the license for this Vocera Voice Server. Speech Ports identifies the number of ports available for speech recognition. Locale identifies a particular cultural, political, or geographic region, which determines several aspects of the Vocera system, including Genie personas, language pack, grammars, and dialing plan. The Spoken Name Count field displays the total number of names that the system can possibly recognize. It includes the names of users, groups, sites, locations, address book entries, and all possible alternate names, such as spellings of user names and the singular and plural names of groups.
User Licenses	n/a	Displays a summary of the user license information for this Vocera Voice Server. It displays the number of User Licenses, Registered Users, Login Licenses, Logged-in Users, Vocera Access Anywhere Licenses, and Vocera Access Anywhere Users. An Enterprise license has unlimited User Licenses and a limited number of Login Licenses. The number of Vocera Access Anywhere Users cannot exceed the number of Vocera Access Anywhere Licenses.
Report Server Licenses	n/a	Displays the type of Report Server license (Not Available, Basic, or Unlimited) and whether the Report Server Scheduler is available.
Other Licenses	n/a	Displays the number of Device Licenses and VMI Licenses.
Application Licenses	n/a	Displays a summary of Vocera application licenses. Each application license has a 2-character ID. The screen displays the number of each type of application license, as well as the number of application licenses that are currently assigned to users. Vocera application licenses can be identified by the following IDs: • VB = Vocera Collaboration Suite for Cisco • UC = Vocera Staff Assignment Premier VA licenses are no longer supported, and the value of this ID is always 0. **Note:** The number of currently configured Staff Assignment Premier licenses is always 0, regardless how many users are currently logged into the application. However, you can log into Staff Assignment as an administrator to identify how many people are actually using Staff Assignment Premier. For more information, see the *Vocera Staff Assignment Guide*. If you need additional Vocera licenses, please contact Vocera.

To display, update system settings, or refresh license information:

1. To display the license information:
   a. Click System in the navigation bar to display the System screen.
   b. Click the License Info tab to display the License Info page.
2. To update system settings for the Vocera licenses:
   a. Enter values in the Company Name and Report Server IP Address fields.
   Choose from:
   • Click Save Changes to save the settings.
   • Click another tab in the System screen to enter additional system settings.
3. To load an updated license:
   a. Click the Refresh License button to upload the new or temporary license to the Vocera Voice Server.
   Note: The license can be refreshed without a Vocera Voice Server restart if the new or temporary license includes an increase in the number of users or IP lines. All other

changes to the license requires a restart. This condition applies to all of the nodes in a cluster environment as well.

Setting Passwords

Learn the password types and necessary steps to set them up in your Vocera environment.

The Passwords page of the System screen lets you maintain default passwords:

- The Administrator Password provides access to the built-in administrator account.

  By default, the Administrator Password is admin. The user ID for this built-in administrator account is Administrator.

- The Initial User Password provides a default password for each new user account. Users can specify this password to gain access to the user Console the first time they log in. Users can then change this initial password.

  By default, the Initial User Password is blank. That is, users do not have to provide a password the first time they log in to the User Console.

- The Initial Phone Password provides a default phone password for each new user account. Users can specify this password to access the Genie from a phone.

  By default, the Initial Phone Password is blank. Users who are enabled to access the Genie from a phone must specify a phone password if Caller ID is not supported.

> **Note:** Initial passwords do not affect *existing* user profiles, only profiles that you create after specifying the initial password.

The Passwords page provides the following fields:

Table 30: Password fields

Field	Maximum Length	Description
Administrator Password	25	Enter a password of five to 25 characters. Letters, digits, spaces, periods, dashes (-), asterisks (*), and underscore characters (_) are allowed. The password is case-sensitive.
Re-enter Administrator Password	25	Re-enter the Administrator password to confirm that you typed it correctly.
Initial User Password	25	Enter a password of five to 25 characters. Letters, digits, spaces, periods, dashes (-), asterisks (*), and underscore characters (_) are allowed. The password is case-sensitive.
Re-enter Initial User Password	25	Re-enter the Initial User password to confirm that you typed it correctly.
Initial Phone Password	25	Enter a password of five to 25 characters. Letters and digits are allowed. Special characters are not allowed. The password is case-sensitive.
Re-enter Phone Password	25	Re-enter the Initial Phone password to confirm that you typed it correctly.

To set default passwords:

1. Click System in the navigation bar to display the System screen.
2. Click the Passwords tab to display the Passwords page.
3. Enter and confirm passwords.
4. Do either of the following:
   - Click Save Changes to save the settings.
   - Click another tab in the System section to enter additional system settings.

> **Note:** In addition to using the built-in administrator account, you can also create a group that has administration permission. Users in this group can access the administration console using their own log in name and password.

Setting System Preferences

The Preferences page of the System screen establishes default settings for the entire Vocera Communications System.

These settings are site-independent—they are basic preferences that determine how the entire Vocera system operates.

To set the system preferences:

1. Click System in the navigation bar to display the System screen.
2. Click the Preferences tab to display the Preferences page.
3. Complete the settings in the Login/Logout Options section as follows:

Table 31: Login/logout settings

Setting	Description
Self Registration	Specifies whether users can add themselves to the Vocera system through the User Console. By default, this setting is not selected.
Login/Logout Voice Commands	Specifies whether to enable the voice commands that allow users to log into and log out of badges. By default, these commands are enabled. This setting is recommended when users share badges. A user can issue a voice command to log out, then give the badge to another user, who can in turn issue a voice command to log in. If you disable these commands, users cannot share badges. In addition, you must manually set the Badge ID for each user in the Edit User dialog box on the Users page of the Administration Console. By default, this setting is selected.
Enable Auto-Logout Period	Specifies whether to log out users automatically when they are off the network for a period of time that you determine. For example, if users leave with their badges and forget to log out at the end of their shifts, you can automatically log them out and make their user licenses available for others. Auto-logout is useful when your user license specifies a maximum number of simultaneous logins. Once you reach this limit, additional users cannot log in. Use this feature in combination with Auto Logout When Badge In Charger in the Defaults section to ensure that users stay logged in only when they intend to be on the network. By default, this setting is not selected.
Auto-logout users after	Specifies the duration of time, in minutes or hours, that must expire while users are off the network before they are automatically logged out. The value you enter cannot exceed 24 hours. The default is 2 hours. **Note:** This field is available only if Enable Auto-Logout Period is selected.

4. Complete the settings in the Department Names In Voice Commands section as follows:

Table 32: Department names in voice commands settings

Setting	Description
First name, Last name and Department	Specifies whether users can utter both the first and last name of a user as well as the user's department. By default, this setting is not selected.
First name and Department	Specifies whether users can utter only the first name of a user as well as the user's department. By default, this setting is selected.

Vocera uses the methods that you select *in addition to* the first and last name, alternate spoken names, and identifying phrase that you specify in the Users tab of the navigation bar.

You must select at least one of these settings to allow users to reference department names in voice commands.

5. Complete the settings in the Favor Frequently Called section as follows:

Table 33: Favor Frequently Called

Setting	Description
Enable for Departments	Enables the use of call history data for calls made from users in one department to users in other groups to enhance speech recognition for the Vocera system. For more information, see **How to Enable Favor Frequently Called for Departments** on page 89. By default, this setting is selected.
Enable for Users	Enables the use of call history data for calls made to a circle of frequently users in to enhance speech recognition for the Vocera system. For more information, see **How to Enable Favor Frequently Called for Users** on page 91. By default, this setting is *not* selected.
None	Disables the Favor Frequently Called feature for users and departments.

6. Complete the settings in the Miscellaneous section as follows:

Table 34: Miscellaneous settings

Setting	Description
Max. Voice Message Length	Specifies the maximum length of voice messages callers can leave for badge users, in seconds. Enter a value between 60 and 180. By default, the value is 60 seconds. **Note:** Audio files can consume a great deal of disk storage on the Vocera drive. One minute of recorded audio requires approximately one megabyte of space.

7. Select a **VMI** preference for whether to prevent VMI messages from breaking through to recipients in Do Not Disturb mode:

Table 35: VMI settings

Setting	Description
Block all VMI messages for users in DND	Blocks all VMI messages—even urgent messages—for users in Do Not Disturb mode.
Block non-urgent VMI messages for users in DND	Blocks non-urgent VMI messages for users in Do Not Disturb mode. Urgent VMI messages will break through Do Not Disturb mode. This is the default setting.
Do not block VMI messages for users in DND	Allows all VMI messages to break through Do Not Disturb mode. This is the default setting.

8. Select a **Vocera Messaging Platform (VMP)** preference:

Table 36: Vocera Messaging Platform settings

Setting	Description
Enable VMP	Specifies whether to enable integration with Vocera Messaging Platform, which provides enterprise messaging and alerting capabilities. When Vocera Messaging Platform is enabled, Vocera users can receive alerts from the Vocera Messaging Platform server on their Vocera devices. When Vocera users say a command to send a page to someone in the Vocera Messaging Platform system, the Vocera Messaging Platform server will route an alert to the appropriate smartphone or pager. By default, this setting is not selected. **Note:** Vocera Messaging Platform should only be enabled after Vocera Messaging Platform has been installed and configured for integration with Vocera Voice Server, and Vocera Messaging Platform address book entries have been imported into the Vocera system. Otherwise, clear the **Enable VMP** box.

9. Do either of the following:
   - Click Save Changes to save the settings.
   - Click another tab in the System section to enter additional system settings.

Setting Sweep Options

The sweep feature lets the Vocera Voice Server clean up voice messages, text messages, and email messages at regular intervals that you specify.

It also removes temporary user accounts on an expiration date that you specify in the Add/Edit User dialog box. When a sweep occurs, the Vocera Voice Server performs the following tasks:

- It deletes messages regardless of whether the user has played or read them, unless they have been saved.
- It deletes all information about a temporary user from the database.

The sweeps are permanent—users cannot access messages after the Vocera Voice Server sweeps them. Similarly, temporary users who have been removed cannot log in after a sweep occurs.

Independent of the sweep mechanism, the Vocera Voice Server also limits the combined total of text and email messages each individual can store or save.

- Each user can **store** up to 20 combined text and email messages at a time. When a user receives a 21st message, the Vocera Voice Server deletes the oldest unsaved message.
- Each user can **save** up to ten of the 20 stored messages.

Table 37: Sweep settings

Section	Description
Sweep Time	In the Sweep Time section, specify the time of the day when you want the sweep to occur. The default sweep time is 1 a.m.
Sweep Age	In the Sweep Age section, specify the amount of time you want to elapse before the Vocera Voice Server sweeps messages. • Enter a number between 1 and 9999 in the text field. • Select either Days or Weeks from the list. The default sweep age is 2 weeks.

To set the Sweep options:

1. Click System in the navigation bar to display the System screen.
2. Click the Sweep tab to display the Sweep page.
3. Enter sweep settings.
4. Do one of the following:
   - Click Save Changes to save the settings.
   - Click Reset to revert to the last saved settings
   - Click another tab in the System screen to enter additional system settings.

Setting Backup Preferences

Learn about the Backup page and restoring system data.

The Backup page of the Administration Console lets you perform the following tasks:

- Specify the number of backup files the system will keep.
- Schedule an automatic backup.

See **Backing up and Restoring Data** on page 160 for information about restoring backed up data or performing a manual backup.

Backup Settings

Whenever your system automatically performs a backup, and when you manually backup your database, Vocera saves your data in a single file in the **\vocera\backup** directory.

Because database backups can be large, Vocera lets you specify the maximum number of backup files to keep. The maximum is the total number of all backup files, regardless of whether they were created automatically or manually. When you exceed the maximum number of files, Vocera deletes the oldest file and saves a new one.

To specify the number of backup files to keep:

1. Click System in the navigation bar.
2. Click the Backup tab to display the Backup page.
3. Enter a number between 1 and 99 in the Maximum number of backup files to save field. The default is 10.
4. Click Save Changes.

Scheduling an Automatic Backup

Learn the steps to setup an automatic backup of your data.

To schedule an automatic backup:

1. Click System in the navigation bar.
2. Click the Backup tab to display the Backup page.
3. Make sure Enable automatic scheduled backups is selected. By default, it is selected.
4. Specify how often you want the automatic backup to occur in the Back up every field. By default, backups occur daily.
5. Specify the time when you want the automatic backup to begin in the Backup time fields. The default backup time is 3 a.m.
6. Click Save Changes.

Setting Text Message Enunciation Properties

When a Vocera device receives an urgent Vocera Messaging Interface (VMI) message, the device plays an alert tone and then immediately plays the message along with the responses (if any) sent with the message.

For all other text messages, a Vocera badge or VCS application plays an alert tone and displays the text of the message; a Vocera smartphone plays an alert tone and prompts you whether to open the message.

There are two properties you can set in the `properties.txt` file on the Vocera Voice Server to control what types of text messages are played immediately on a badge or a Vocera smartphone:

- MsgEnuciateModeSmartphone – controls whether text messages received on Vocera Smartphones (Wi-Fi phones manufactured by Motorola) are played immediately. This property does not affect Vocera badges.
- MsgEnunciateMode – controls whether text messages received on Vocera badges or smartphones running Vocera Connect are played immediately.

The following table summarizes how the setting of these properties affects enunciation:

Value	Enunciated messages
0	Urgent VMI messages, high-priority VMP alerts, and urgent text messages sent by email. This setting is the default.
1	All urgent text messages.

Value	Enunciated messages
2	All VMI messages. Urgent messages continue to take priority. Their enunciation interrupts other messsages and does not allow interruption by lower-priority messages; instead, lower-priority messages are delivered but not enunciated.
3	All text messages. Urgent messages continue to take priority. Their enunciation interrupts other messsages and does not allow interruption by lower-priority messages; instead, lower-priority messages are delivered but not enunciated.
4 - 9	None.

To set text message enunciation properties:

Learn how to set text messages enunciation properties.

1. On each Vocera Voice Server node, open the `\vocera\server\properties.txt` file in a text editor.
2. Add the MsgEnunciateMode and MsgEnunciateModeSmartphone properties (if they have not already been added).

   Set each property to a value of 0 through 9, as described in **Setting Text Message Enunciation Properties** on page 112.

   For the MsgEnunciateMode property, you can also choose to enter a comma-delimited list to control text message enunciation for each VMI application or site. See **Specifying MsgEnunciateMode Per VMI Client or Site** on page 113.
3. Save the `properties.txt` file.
4. Stop the Vocera Voice Server and start it again. The Vocera Voice Server loads `properties.txt` into memory.

   Note: If you have a Vocera Voice Server cluster, stop and start the standby nodes first, and then switch to the active node and choose Cluster > Failover in the Vocera Control Panel.

Specifying MsgEnunciateMode Per VMI Client or Site

The MsgEnunciateMode property allows you to enter a comma-delimited list of values to specify the enunciate mode for a VMI client, a site, or both.

This helps you control which text messages are enunciated for each VMI application or site.

Each item in the comma-delimited list consists of three subitems delimited by colons:

ClientID : SiteName : EnunciateMode

where

- ClientID = The unique Client ID for a VMI application (optional, can be left blank)
- SiteName = The current site of the recipient of the message (optional, can be left blank)
- EnunciateMode = A one-digit numeric value representing the enunciate mode, described in **Setting Text Message Enunciation Properties** on page 112

The server processes the MsgEnunciateMode property from left to right using the following rules:

- The MsgEnunciateMode property values must be on one line. Values that run onto another line are ignored.
- A blank ClientID or SiteName subvalue serves as a wildcard.

  In the next value, the ClientID is blank, which means the value applies to all VMI client IDs:

  ```
  San Jose:1
  ```

  In the next value, the SiteName is blank, which means the value applies to all sites:

  ```
  Connexall::1
  ```

- A more specific value always takes precedence. For example, the value `Emergin:San Jose:1` takes precedence over `San Jose:2`.
- If there is a tie between two values, the leftmost value takes precedence. For example, there is a tie in the following two values, so the first one is used:

  ```
  Emergin:Santa Cruz:0, Emergin:Santa
  Cruz:4
  ```

- If a value cannot be resolved (for example, the ClientID and SiteName are specified incorrectly or the EnunciateMode is missing), the default EnunciateMode value, 0, applies.
- If you omit the optional ClientID and SiteName subvalues, you can also omit the colons. For example, the following values are all valid:

  ```
  1, San Jose:3, Emergin::4
  ```

- Examples

  `MsgEnunciateMode = 0, San Jose:3, Emergin:San Jose:4`

  The following text messages are enunciated:

  - All urgent VMI messages (0).
  - All text messages received by users in San Jose ("San Jose:3"), except those sent by Emergin, which are NOT enunciated ("Emergin:San Jose:4").

  `MsgEnunciateMode = 0, San Jose:1, Santa Clara:1, Emergin:San Francisco:2, ConnexAll:Palo Alto:2, Cupertino:3, Santa Cruz:4`

  > **Note:** For the purposes of this example, the MsgEnunciateMode property spans multiple lines. However, in the actual `properties.txt` file, the MsgEnunciateMode property must appear on one line.

  The following text messages are enunciated:

  - All urgent VMI messages (0).
  - Urgent text messages received by users in San Jose ("San Jose:1")
  - Urgent text messages received by users in Santa Clara ("Santa Clara:1")
  - VMI text messages with the VMI client ID "Emergin" received by users in San Francisco ("Emergin:San Francisco:2")
  - VMI text messages with the VMI client ID "ConnexAll" received by users in Palo Alto "ConnexAll:Palo Alto:2")
  - All text messages received by users in Cupertino ("Cupertino:3")

  All text messages received by users in Santa Cruz are NOT enunciated ("Santa Cruz:4").

Other Hidden Properties

Learn about the properties that are updated manually in the `properties.txt` file.

When making updates using the Vocera Administration Console, some of your selections cause updates to the `properties.txt` file under the covers. However, there are some properties that cannot be enabled using the Adminstration Console. These properties are known as "hidden" since they are not appearant to the user.

The Vocera Voice Server supports these additional hidden properties. The `properties.txt` is located in `\vocera\server\properties.txt`. After you updated the `properties.txt` file, be sure to restart the server to enable or disable the new setting.

> **Note:** Vocera recommends calling Customer Support if you plan to manually update the `properties.txt` file.

Table 38: Hidden properties

Property	Description
IPVMISecureEnable	Enables secure VMI support within the Vocera Voice Server. When this property is set to TRUE the Vocera Voice Server opens a port to listen for secure VMI client connections. The default is FALSE.
IPVMISecureListeningPortNo	Specifies the port the Vocera Voice Server uses to listen for secure VMI client connections. The default is port 5007.
MsgDisableSkipMessageResponse	Enter **true** (the default) or **false**. Set to **true** to disable the "Skip" response for VMI messages that are played aloud, forcing users to say a valid response, such as "Accept" or "Reject." Set to **false** to enable the "Skip" response. For details, see the Vocera Messaging Interface.
SysBroadcastResponse	Enables or disables responses to broadcasts. Enter **true** (the default) or **false**. To make broadcasts uninterruptible, set this property to **false**.
SysLoginLicenseAlertThreshold	If there is a login license limit, this property sets the percentage threshold at which the Vocera Voice Server will send an email alert whenever the threshold is exceeded. Enter a decimal value. The default threshold is .90 (90%) of the login license limit. For example, to increase the alert threshold from 90% to 95%, enter **.95**.
SysMaxRejectedLogins	Sets the maximum number of rejected login attempts before the user is prevented from logging in from that machine for one minute or the interval specified by the **SysMaxRejectedLoginsPeriod** property. Enter any positive integer.
SysMaxRejectedLoginsPeriod	Sets the time period (in milliseconds) that a user is prevented from logging in from a machine on which he has reached the maximum number of rejected login attempts. Enter any positive integer (the default is 60000 milliseconds, or 1 minute).
SysFunnyGenie	Enables or disables the funny Genie. Enter **true** (the default) or **false**.
VMIBroadcastEnabled	You no longer need to set this property for urgent Broadcast messages to large groups. The Vocera Voice Server has been enhanced so that unicast messages always utilize a single speech port. For details, see the *Vocera Messaging Interface Guide*.
VMIResponseMapping	Maps VMI responses passed from a middleware system to other response choices. For details, see the *Vocera Messaging Interface Guide*.
VMIResponseTimeout	Enter the number of seconds that a user can be prompted to respond to a new alert or alarm before the message times out. For details, see the Vocera Messaging Interface.

Property	Description
VMITimeoutResponse	Enter the response that is used when a new alert or alarm reaches the specified VMIResponseTimeout. For details, see the Vocera Messaging Interface.
VMITouchCallResponse	Enter the Vocera response phrase that is used when a user presses the Call button to respond to a new VMI message. For details, see the Vocera Messaging Interface.
VMITouchDNDResponse	Enter the Vocera response phrase that is used when a user presses the DND button to respond to a new VMI message. For details, see the Vocera Messaging Interface.
VMITouchCallHoldResponse	Enter the Vocera response phrase that is used when a user presses and holds the Call button to respond to a new VMI message. For details, see the Vocera Messaging Interface.

Note: If you modify the `properties.txt` file, you must stop and start the Vocera Voice Server to load the properties into memory.

Creating Custom Quick Notes for Smartphone Users

When you type a text message on the Vocera smartphone, you can display a list of Quick Notes, commonly-used phrases and expressions.

You can select one of the Quick Notes to insert it into the message, saving you from typing the text.

The Vocera system administrator can customize the Quick Notes list, adding phrases or expressions that your organization commonly uses. The Quick Notes list is common to all Vocera users. Individual users cannot create a personal Quick Notes list.

By default, the Quick Notes list on the Vocera smartphone includes the following phrases:

- Yes
- No
- OK
- Call me back
- Need help
- Where are you?
- Will call you later
- Busy
- On my way
- Thank you
- Need more info
- Can this wait?

To create a custom Quick Notes list for all Vocera smartphone users:

1. In a text editor, enter each note on a separate line.

   Limit each note to 100 characters. That is the maximum number of characters you can enter into a text message on the smartphone.

   Do not add more than 15 notes to the list. Otherwise, users may find the list too long to be helpful.

2. Save the document to a file named `quicknotes.txt`.

3. Copy the `quicknotes.txt` file to the following folder on the Vocera Voice Server. If you have a Vocera cluster, copy the file to every Vocera Voice Server node.

`\vocera\data\applications\contacts`

4. Choose Start > Settings > Control Panel > Administrative Tools > Services. **The Services window appears.**

5. Stop the Tomcat service and then start it again.

6. Close the Services window.

> **Note:** The `quicknotes.txt` file is NOT synchronized continuously with Vocera cluster nodes, unlike Vocera Voice Server database transactions. However, the file is automatically copied from the active Vocera node to standby nodes during a remote restore.

Setting System Defaults

Defaults are Vocera system settings that apply to users at all sites, such as the greeting used by the Genie or the ring tone used to announce a call.

An override setting for each default determines whether users can customize the setting you specify, or whether the system default takes precedence over a user preference.

Overriding User Settings

You can use the Defaults screen in the Administration Console to change a default setting at any time.

Changes update the server as soon as you save them, but they do not affect existing users unless you set Override User Settings to Yes. By default, Override User Settings is set to No for all default settings.

The overrides let you establish baseline system settings at any time. For example, to turn off the alert tones that announce a text message, you would deselect the **Text Message Alert** property on the Notifications page and set **Override User Settings** for that property to **Yes**. This change would affect all new and existing users.

If you later want to allow users to customize this property, set **Override User Settings** for the **Text Message Alert** property to **No**. The alert tones for all users remain turned off until they manually enable them again.

Choosing Genie Settings

Learn about Genie settings and how to create them in your Vocera environment.

The Genie is the voice interface between the user and the Vocera Voice Server. When a user presses the Call button on a badge, the Genie sends a greeting, accepts commands, and, when necessary, prompts the user. When a call or a message comes to the badge, the Genie notifies the recipient.

Table 39: Genie settings

Setting	Description
Genie Persona	A Genie persona is a set of voice prompts and tones that give the voice interface a distinctive identity. Click a radio button to choose a persona. Click the icon by a persona name to play a sample. The default Genie Persona varies per locale, and Override User Settings is set to No.
Genie Greeting	A badge plays the Genie greeting when a user presses the Call button. Click a radio button to choose one of the following settings: Tone Only, Speech Only ("Vocera"), or Tone and Speech. Click the icon by a choice to play a sample. By default, the selected Genie Greeting is Speech Only, and Override User Settings is set to No.

Setting	Description
Call Announcement	In the Call Announcement section, choose a Ring Tone from the list. Click the icon by a tone to play a sample. By default, the selected ring tone is Ring-Tone-01, and Override User Settings is set to No.
Announce Caller's Name After Tone	If you want the user to hear who is calling, select Announce Caller's Name After Tone. This announcement adds to the time required to connect each call. By default, the Announce Caller's Name After Tone box is selected, and Override User Settings is set to No.
Announce Name of Called Group	For calls made to a group, if you want the Genie to identify the group that was called and the group's site (if it is different from the caller's site) to set the context of the call for the recipient, select Announce Name of Called Group. Instead of saying, "[CallerName]. Accept call?" to announce the call, the Genie says, "Call to [GroupName] from [CallerName]. Accept?" This announcement adds to the time required to connect each call. If the caller and the called group are from different sites, the Genie says, "Call to [GroupName] at [SiteName] from [CallerName]. Accept?" By default, the Announce Name of Called Group box is selected, and Override User Settings is set to No.

To choose Genie settings:

1. Click Defaults in the navigation bar.
2. Select the Genie Setting tab to display the Genie Settings page.
3. Specify Genie settings.
4. Click Save Changes.

Choosing Badge Notifications

Badge Notifications specify the alert tones and reminders that badges play, and determine which automatic badge features are enabled in user profiles.

Specify alert tone settings in the Alert Tones section:

Table 40: Alert tones settings

Setting	Description
On/Off Network Alert	On/Off Network Alert plays a tone when the user moves out of the range of the wireless network. The audible warning is a convenient reminder if users are supposed to leave badges behind when they go home. However, if users routinely move between buildings, and the network does not cover the outdoor spaces, they might not want to hear an alert tone. By default, the On/Off Network Alert box is selected, and Override User Settings is set to No.
Low Battery Alert	Low Battery Alert sounds an alert when the battery needs to be recharged. By default, the Low Battery Alert box is selected, and Override User Settings is set to No.
Text Message Alert	Text Message Alert plays a tone when the user receives a new text message. The tone sounds only once for each new message. An envelope icon also appears on the badge display when the user has unread text messages. By default, the Text Message Alert box is selected, and Override User Settings is set to No.
Voice Message Alert	Voice Message Alert issues a tone when the user receives a new voice message. The tone plays only once for each new message. A telephone icon also appears on the badge display when the user has unplayed voice messages. By default, the Voice Message Alert box is selected, and Override User Settings is set to No.
Disable Alert Tones in DND Mode	Disable Alert Tones in DND Mode prevents all alert tones when a user puts the badge in Do Not Disturb mode. By default, the Disable Alert Tones in DND Mode box is cleared, and Override User Settings is set to No.

Choose any reminders you want to enable in the Reminders section:

Table 41: Reminders settings

Setting	Description
Text Message Reminder	Select Text Message Reminder to play a tone on the badge every 15 minutes until a user picks up new text messages. By default, the Text Message Reminder box is cleared, and Override User Settings is set to No.
Voice Message Reminder	Select Voice Message Reminder to play a tone on the badge every 15 minutes until a user picks up new voice messages. By default, the Voice Message Reminder box is selected, and Override User Settings is set to No.
DND Reminder	Select DND Reminder to play a tone on the badge every 15 minutes when the badge is in Do Not Disturb mode. By default, the DND Reminder box is selected, and Override User Settings is set to No.

Choose any notifications you want to enable in the Automatic Notifications section. Automatic notifications allow users to bypass certain operations without confirming them.

Table 42: Automatic notifications settings

Setting	Description
Auto Logout When Badge in Charger	Auto Logout When Badge in Charger sends a message to the Vocera Voice Server to log the current user out when a badge is placed in a battery charger, and then turns off the badge's power. This is useful when people share badges, because a user whose badge has a low battery can place the badge in an eight-bay charger, take a fully charged badge out of the charger, and immediately log in with the charged badge. If Auto Logout When Badge in Charger is disabled, the badge power for an active badge remains on, and the user stays logged in to the server while the battery is charging. This is convenient when a user is working at a desk and wants to use the badge while it is in a single-bay charger. By default, the Auto Logout When Badge in Charger box is selected, and Override User Settings is set to No. **Note:** This setting does not affect B3000 badges, which cannot be placed in a charger.
Auto Answer for Incoming Calls	Auto Answer for Incoming Calls connects callers immediately, without asking users whether or not they want to take the call. If all calls need to be connected quickly, you can enable this feature. By default, the Auto Answer For Incoming Calls box is cleared, and Override User Settings is set to No.
Missed Call Notification	Missed Call Notification causes the Genie to notify the user of missed calls since the last time the user pressed the Call button. The Genie also announces the names of people who left messages. By default, the Missed Call Notification box is selected, and Override User Settings is set to No.
Disable Voice Message Notifications	Disable Voice Message Notifications causes the Genie to suppress notifications when a user receives a message. However, the user may still hear a voice message alert tone (if the Voice Message Alert option is selected), and a telephone icon appears on the badge display when the user has unplayed voice messages. By default, the Disable Voice Message Notifications box is selected, and Override User Settings is set to No.

To choose Badge Notifications:

1. Click Defaults in the navigation bar.
2. Click the Notifications tab to display the Notifications page.
3. Specify badge notification settings.
4. Click Save Changes.

Choosing Miscellaneous Settings

Enter settings in the Miscellaneous page to control the behavior of the Play Messages commands, the call setup, and the enabling of Vocera Access Anywhere.

Table 43: Miscellaneous settings

Setting	Description
Play Messages Oldest First	Play Messages Oldest First causes messages to be played back in the order in which they were received. Urgent messages are always played before non-urgent messages, regardless of this setting. By default, the Play Messages Oldest First box is cleared, and Override User Settings is set to No.
Play Voice Message Time and Date	Play Voice Message Time and Date causes the playback of each voice message to be preceded by the time and date the message was sent. If you don't choose this option, users can still hear the date and time a message was sent by pressing the Call button and saying "Date" or "Time" during or just after the play of the message. By default, the Play Voice Message Time and Date box is selected, and Override User Settings is set to No.
Play Text Message Time and Date	Play Text Message Time and Date causes the playback of each text message to be preceded by the time and date the message was sent. If you don't choose this option, users can still hear the date and time a message was sent by pressing the Call button and saying "Date" or "Time" during or just after the play of the message. By default, the Play Text Message Time and Date box is cleared, and Override User Settings is set to No.
Fast Call Setup	If you select Fast Call Setup, the call is connected as soon as the recipient accepts it rather than after the call announcement to the caller is finished. With Fast Call Setup selected, the recipient of a call hears, "[CallerName], Accept Call?". Meanwhile, the caller hears the name of the recipient. If the call is forwarded to a phone, the caller hears the forwarding announcement before the call is connected. If you do not select Fast Call Setup, the Genie always completes the call announcement to the caller before connecting the call. If the recipient has a long name, this can cause a brief delay before the call is connected. By default, the Fast Call Setup box is selected, and Override User Settings is set to No.
Announce Through Speaker	Use the Announce Through Speaker setting to specify the way the badge plays call and message announcements when headsets (or managed lanyards) are used: Select Announce Through Speaker to play incoming call and message announcements through the badge speaker when a headset is plugged in. If you select this feature, only the *announcement* plays through the speaker; the actual call or message then plays through the headset. Clear Announce Through Speaker to play both the announcement and the call or message through the headset. When a headset is plugged into the badge, all audio plays through the headset by default. Consequently, if users don't wear their headsets all the time, they may not hear an incoming announcement, and they may not know that someone is trying to contact them. If you select Announce Through Speaker, users can leave their headsets plugged in, and simply put them on to communicate after they hear the announcement. If Announce Through Speaker is turned on and users are wearing their headsets when a call comes in, they may not hear an announcement in a noisy environment (because it plays through the speaker); however, they will still hear the call or message through the headset. When a headset is not plugged in, all calls, messages, and announcements play through the speaker, as usual, regardless of the Announce Through Speaker setting. By default, the Announce Through Speaker box is selected, and Override User Settings is set to No.
Accept Calls Using Buttons Only	Requires users to accept or reject incoming calls by pressing the Call or DND/Hold button. Selecting this feature disables the use of "Yes" and "No" voice commands to accept and reject incoming calls. This feature is useful in certain high-noise environments. Vocera allows users to accept or reject a call with either voice commands or buttons. In some situations, background noise can cause poor speech recognition, resulting in the Genie repeatedly saying "I'm sorry, I didn't understand". In other situations, background noise can cause the Genie to prematurely accept or reject calls without user input. To avoid these problems, select this box to require users to answer calls using buttons only.

Setting	Description
	By default, the Accept Calls Using Buttons Only box is cleared, and Override User Settings is set to No. Enabling this feature establishes a new system-wide default and may require re-training.
Enable Access to Genie from Phone	Important: Unless you have enough Vocera Access Anywhere licenses for all of your users, Vocera recommends that you leave this default setting cleared.
	When this option is selected, it enables the ability for users to access the Genie from a standard telephone to perform Vocera functions other than basic calling. For example, you can phone the Vocera Direct Access number, and say a command to the Genie to broadcast a message to a group or play your messages.
	The number of users that can use the Vocera Access Anywhere feature is controlled by your Vocera license. If you don't have the license, Vocera Access Anywhere is not supported. Even with the proper license, only users that have been specifically enabled to use the Vocera Access Anywhere feature can take advantage of it.
	By default, the Enable Access to Genie from Phone box is cleared, and Override User Settings is set to No.

To set miscellaneous options:

1. Click Defaults in the navigation bar.
2. Click the Miscellaneous tab to display the Miscellaneous page.
3. Specify settings.
4. Click Save Changes.

Choosing Advanced Speech Settings

Enter settings in the Advanced Speech Settings page to change the defaults for the Favor Frequently Called feature for users.

Table 44: Advanced speech rec settings

Setting	Override User Settings (Defaults)
Enable for All Users = **Selected**	• **Yes**: Frequently called users is *enabled* for all users in your environment. • **No**: Frequently called users is *enabled* for all users in your environment but you can disable it for individual users on the User > Edit Users > Speech Rec page.
Enable for All Users = **Not Selected**	• **Yes**: Frequently called users is *disabled* for all users in your environment. • **No**: Frequently called users is *disabled* for all users in your environment but you can enable it for individual users on the User > Edit Users > Speech Rec page.

To change default settings for the Frequently Called feature for users:

1. Click Defaults in the navigation bar.
2. Click the Advanced Speech Settings tab to display the Advanced Speech page.
3. Specify settings.
4. Click Save Changes.

Configuring and Managing Clusters

Use the Cluster Setup page of the System screen to configure and manage a Vocera Voice Server cluster. Vocera supports up to four machines in a cluster.

The Cluster Setup page lets you perform the following tasks:

- Specify the external IP address for each Vocera Voice Server machine that is used by Vocera Collaboration Suite clients to connect to the server.
- Configure two or more individual servers to work together as a single Vocera cluster.
- Manage an existing cluster.
  - Add a server to an existing cluster.
  - Edit the information for one of the nodes in a cluster.
  - Remove a server from a cluster.
  - Change the failover priority of servers in the cluster.
  - Fail over the active server.

About Vocera Voice Server Clusters

Learn concepts related to Vocera Voice Server clusters.

Some environments require redundancy to support critical applications in the event of hardware or software failure. In such environments, a critical application is installed on two or more computers. The computer controlling the application is called the *active* node, and the other computers are called the *standby* nodes. This redundant combination of active and standby nodes is called a *cluster*.

Vocera clustering provides high availability when any of the following events occur:

- The computer hardware fails.
- The Vocera Voice Server fails.
- The Nuance service fails.
- The MySQL service fails.

The cluster's active node controls the Vocera system, but a standby node can take over control of the application if the active node fails. The situation where a standby node takes control from the active node is called a *failover*.

The telephony integration option (Vocera SIP Telephony Gateway, if installed, should run on a server that is separate from the Vocera cluster so telephony support can continue if the Vocera Voice Server fails over. Failover for the telephony server itself is supported as part of the high availability architecture.

The following figure shows the way that the Vocera SIP Telephony Gateway, the Vocera Report Server, and badges connect to a Vocera cluster:
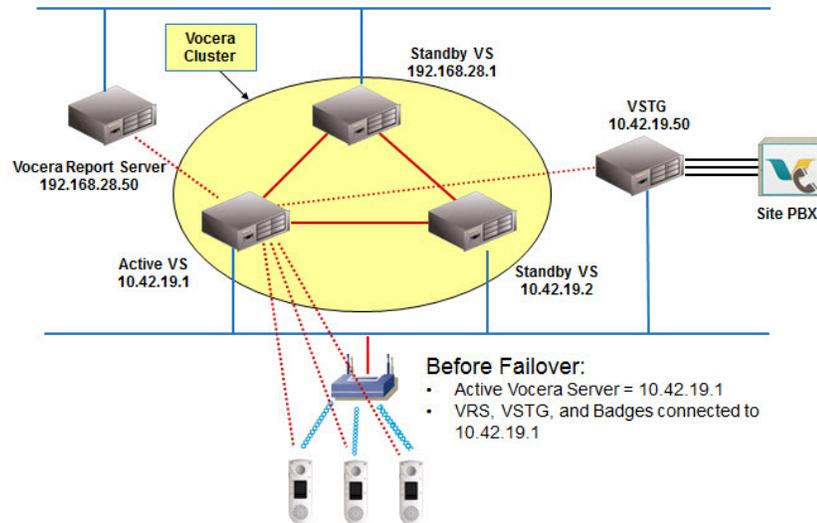
Figure 11: Vocera Cluster Before Failover

As shown in the above illustration, the nodes in a Vocera cluster do not share a single virtual IP address, as they would with the Microsoft Cluster Service. Instead, the badges, the Vocera SIP Telephony Gateway, and the Vocera Report Server are all associated with `10.42.19.1`, the IP address of the *active* Vocera Voice Server. Similarly, any Administration Console or User Console sessions would also point to the IP address of the active Vocera Voice Server.

Vocera supports a maximum of four cluster nodes (one active node and three standby nodes). Each cluster node maintains its own copy of the Vocera database, the Vocera Report Server log files, and the `badge.properties` file. The cluster synchronizes these files continually.

If a failover occurs, one of the standby nodes becomes active and takes control of the cluster. At that time, the badges, the Vocera SIP Telephony Gateway, and the Vocera Report Server automatically associate with the IP address of the newly active node, as shown in the following illustration:
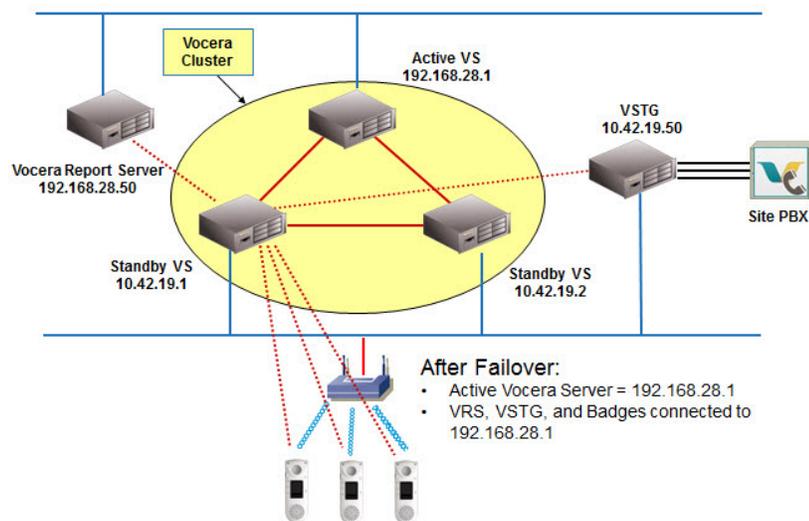
Figure 12: Vocera Cluster After Failover

As shown in the above illustration, Vocera Voice Server nodes, the Vocera SIP Telephony Gateway, and the Vocera Report Server can reside on different subnets. In a Vocera cluster, the Vocera Voice Server and all its related services are always running on any standby nodes so failover can occur quickly. If the active node fails, a standby node becomes active and takes control of the cluster almost immediately.

You can use the Administration Console or the Vocera Control Panel to determine which node of a cluster is active:

- The Vocera Control Panel displays a status message to indicate whether its server is in active or standby mode.

  See "Determining the Status of a Server" in the *Vocera Installation Guide* for complete information.

- The Address field of your web browser displays the IP address of the active Vocera Voice Server.

Because each node maintains an independent copy of the database, the Vocera cluster architecture allows disaster survival. The use of multiple nodes will also allow rolling upgrades with minimal down-time in the future.

Discovery Mode

A cluster member uses *discovery mode* to determine whether it should come online as the active node or a standby node.

A cluster member enters discovery mode in any of the following situations:

- The first time it comes online as a cluster member.
- Any time it does a full restart.
- Any time it loses contact with the active node.
  - If it cannot find a network route to the active node.
  - If the active node fails to service a poll from a standby node.

Each standby node in a cluster polls the active node periodically to draw down synchronization transactions. If the standby node does not receive a response within 10 seconds, it assumes the active node has failed and it goes into discovery mode to find out the status of other nodes in the cluster.

After entering discovery mode, a server takes one of the actions shown in the following table, depending on the status of the other cluster members:

Table 45: Discovery mode actions

Status of other Cluster Members	Action Taken by Server in Discovery Mode
One cluster member is already active.	The server comes online as a standby node.
No cluster member is active *and* no other server is in discovery mode.	The server comes online as the active node and takes control of the cluster.
No cluster member is active *and* one or more other servers are in discovery mode.	The rankings on the Cluster Setup page of the Server screen serve as a tie-breaker.

Sequence of Failover Events

When a failover occurs, a new node becomes active and takes control of the cluster almost immediately.

The telephony server connects to the new active node several seconds later and then becomes available for calls. Badges try to find each server in their cluster list until they locate the new active node and connect to it. The entire system—Vocera Voice Server, telephony server, and badges—becomes available a few seconds after a failover occurs.

Following is the sequence of events that occur during a failover:

1. The Vocera Voice Server on the active node fails, resulting in the following events:
   - The Vocera Control Panel on this failing node closes and the command window displays the message Restarting All Processes.
   - If the badge is in a call with another badge, both badges drop the call within 30 seconds. Badge-to-badge calls often persist for a short while after the active node fails because the server is not directly involved in the call after the initial set up.
   - If the badge is in a call with a phone, the badge drops the call immediately, and the phone drops the call after the telephony server connects to the new active server (within about 30 seconds).

2. Standby nodes continue to look for the most recently active node at 3-second intervals and find out that it is not responding.

3. When the active node does not respond, standby nodes go into discovery mode to determine the status of the other cluster nodes.

4. The first node to enter discovery mode becomes active and takes control of the cluster. If you have configured mail server connectivity, the new active node sends an alert as described in **Cluster Email Notifications** on page 130.

   If multiple nodes are in discovery mode at the same time, the node at the top of the list on the Cluster Setup page of the Server screen becomes active and takes control of the cluster.

5. Badges and the telephony server look for the servers in their cluster list until they find the new active node and then connect to it.
   - When you first configure the Vocera SIP Telephony Gateway, specify the current active cluster node or the list of cluster members. Since the telephony server stays in contact with the cluster, it dynamically maintains the cluster list when nodes are added and removed.
   - When you first configure the badges, you specify the current active node or the list of cluster members. You must then maintain this cluster list in `badge.properties` when cluster nodes are added and removed.

     Because badges are mobile, they can be off-network when the cluster membership changes. However, as long as a badge can locate any current cluster node—even if it is not the active node—it can still connect to the active node and download the current cluster list in `badge.properties`.

6. The Vocera Voice Server that failed restarts, goes through the discovery process, and comes online as a standby node.

Badges and Clusters

Learn how the badge and server interact in the cluster environment.

When badges come online, they attempt to connect to the first server in the cluster list. If that server is not active, they continue sequentially through the list until they find the active node. Badges maintain the IP address of each cluster node along with other data in the `badge.properties` file. Badges will cycle through this list repeatedly, if necessary.

Similarly, if the Vocera Voice Server fails over, badges display "Searching for server" and cycle through the list of IP addresses until they find the active node.

You can set up your badges with the complete cluster list if you know it at the time of initial badge configuration. If you are uncertain of the complete list, you must specify at least one valid cluster IP address. The badge will find the node that you specify, and if it is not active, it will redirect the badge to the active node. See the *Vocera Device Configuration Guide* for additional information.

After badges have received the initial list of cluster members, you can maintain it by updating the `badge.properties` file on the active node. See the *Vocera Device Configuration Guide* for additional information.

Data Synchronization

Each standby node automatically synchronizes its data with the data on the active node to ensure that it is constantly ready to take control of the cluster.

The standby nodes perform two types of synchronization:

- A *remote restore* synchronizes all the data on the standby node with the active node. It occurs the first time a standby node comes online, any time a cluster member comes out of discovery mode as a standby node, and any time the Vocera Control Panel stops and restarts the active node.

  A remote restore reads data directly from the database and does not require a backup file.

  > **Note:** Stopping and starting the active node *does not* cause a failover; however, it *does* cause the standby node to perform a remote restore when the active server restarts.

- *Ongoing updates* synchronize the data on the standby node with any changes that occur after the most recent remote restore. The active node records all database transactions that occur after the remote restore starts in a queue, and the standby node uses the queue to update its database.

In addition, a few special files are synchronized outside the remote restore and ongoing updates processes. The following table provides details about how the various types of files used by Vocera are synchronized:

Table 46: Synchronized files

Type of Data	Synchronization Details
The configuration database	• Completely updated during remote restore. • Kept in sync incrementally during ongoing updates.
Text, voice, and email messages	• Completely updated during remote restore. • Kept in sync incrementally during ongoing updates.
All user recordings, such as learned names, learned commands, and so forth	• Completely updated during remote restore. • Kept in sync incrementally during ongoing updates.
Vocera Report Server logs	• Existing log files are copied to standby nodes during remote restore. • The current log file is copied to standby nodes at one-minute intervals, independently of remote restore. • The current log file is copied to the standbys when the Vocera Voice Server closes the file. • If a failover occurs, the current log file is never more than one minute old, and all previous log files are already on the standby nodes.
The `badge.properties` file	• Copied to standby nodes during remote restore. • Loaded into memory automatically when a standby node becomes active. Best Practice: Modify `badge.properties` on the active node, and then restart the active node. This action loads `badge.properties` into memory on the active node and forces the standby nodes to perform a remote restore and synchronize it.
Backup files	• Backup files are synchronized outside the remote restore and ongoing updates processes. • Standby nodes perform a backup whenever the active node performs a backup. More efficient than copying large zip files across the net. Best Practice: Perform a backup after bringing the cluster online. All nodes will then start with the same backup file.

Several types of files are intentionally not synchronized by the Vocera Voice Server during any process. The following table provides details about these files:

Table 47: Unsynchronized files

Type of Data	Reason not Synchronized
The `properties.txt` file	• Each Vocera Voice Server may require hardware-dependent settings in `properties.txt`. • Each Vocera Voice Server may require different logging parameters in `properties.txt`.
Vocera Voice Server logs	• Every node creates its own set of server logs. The logs are specific to each node and the state it is in at any given time. • Nodes communicate constantly and often log similar events. For example, the logs of both the standby and active node record that the standby node performs a remote restore. Similarly, the logs of both nodes record when a standby node rejoins a cluster after completing a remote restore.
Third-party (Tomcat, Apache, MySQL, and Nuance) logs	• Logs provide details for troubleshooting the specific application on the specific server. • Processes are not managed by the VS cluster communication. • Files are not relevant from one machine to another.

Synchronizing Extensive Changes

Learn about propagating changes on standby nodes and remote restores.

As discussed in Data Synchronization on page 128, remote restores and ongoing updates are the two basic mechanisms the Vocera Voice Server uses to synchronize data among cluster nodes. The Vocera Voice Server performs this synchronization automatically; however, there are times when you may want to *force* the standby nodes to perform a remote restore for the following reasons:

• *Ongoing updates* are effective for propagating incremental changes to standby nodes.

  For example, adding and removing users, changing group permissions, and so forth.

• *Remote restores* are more efficient for synchronizing large sets of changes to the database.

  For example, importing 5,000 entities, updating users with a spreadsheet, transferring site data, and so forth.

The remote restore is effective for large sets of changes because it reads the entire database of the active node into a standby node's memory in a single operation, and then writes it to the standby node's disk. The ongoing updates process treats every edit as a separate operation.

> **Tip:** Use the remote restore mechanism to synchronize large sets of changes. Using remote restore avoids having the standby nodes out-of-sync for long periods of time, and it avoids creating excessive network traffic.

To use a remote restore to force synchronization to occur:

1. Back up your database.

   This action also causes standby nodes to perform a backup.

2. After the backup completes, stop the standby nodes.

3. Perform all the necessary updates on the active node.

   > **Note:** The active node remains running, and the badges remain connected to it.

4. Restart the standby nodes.

   The standby nodes automatically perform a remote restore, synchronizing data quickly.

Similarly, when you first set up a cluster, the best practice is to fully configure the database on the active node, and then bring the standby nodes online. Avoid joining the standby nodes to the cluster before importing large datasets or performing other data-intensive operations. Such operations cause extensive and continual ongoing updates to occur.

Note: In extreme cases, performance degradation from extensive ongoing updates may interrupt communications between a standby node and the active node. If a standby node loses contact with the active node for more than 10 seconds, it will go into discovery mode. At that point, however, it will find the active node, come out of discovery mode as a standby again, and then perform a remote restore.

Performing a Manual Restore from a Backup File

You can use the Administration Console of the active node to restore Vocera Voice Server data manually from a backup file.

The restore operation causes the following events to occur:

- The active node briefly stops.
- The active node empties all its data.
- The active node completely restores data from the backup file.
- The Vocera Voice Server automatically logs out all badges.
  Users must log in again after the restore completes.
- The standby nodes wait for the manual restore to complete, then perform a remote restore to synchronize their data once again.

See Backing up and Restoring Data on page 160 for additional information.

Cluster Email Notifications

You can configure your system to send email alerts to notify you when significant events affect your cluster.

Vocera provides the following cluster-related email messages:

- "Warning: Failover occurred on Vocera cluster. New active server has host name *<IP address>*."
  The new active cluster node sends this message to notify you that a failover has occurred.
- "Standby cluster member *<IP address>* is no longer active. Reported by active server *<IP address>*."
  The active cluster node sends this message to notify you that it has lost contact with a standby node.
- "Warning: Your Vocera Voice Server cluster had multiple active nodes. The server that was active the longest [*<IP address>*] is still active. The other one [*<IP address>*] has automatically reverted to standby mode."
  The active cluster node sends this message to notify you that Vocera has automatically healed a split brain state. If a split brain occurs, you will receive other email messages before this one, as described in Troubleshooting Network Problems and Clusters on page 133.

In environments with an unstable network, these email messages may be symptoms of underlying problems you need to address. See Network Problems and Clustering on page 131 for additional information on interpreting these messages.

Use the Email screen of the Administration Console to configure email alerts. See Email Setup on page 175 and the Administration Console online help for complete information.

Tip: If you implement a cluster, configure email alerts to help you monitor its health. Specify an alias that sends email to the Vocera administrator, an IT person, and anyone else who should know about significant cluster events.

Network Problems and Clustering

The flexibility of a distributed cluster architecture requires you to have a stable network environment.

Vocera clustering provides a distributed architecture that allows you to locate nodes anywhere on your network, including different subnets (as described in About Vocera Voice Server Clusters on page 124) and different geographic locations (as described in Geographically Distributed Clusters on page 136). This flexibility is intended in part to provide disaster recovery capabilities from catastrophic events such as an earthquake or a WAN failure.

In particular, either of the following network problems will cause unwanted cluster behavior:

- Network outages

  For Vocera purposes, any network event that blocks all routes between the active node and a standby node is an outage. For example, restarting a switch may cause an outage.

- Excessive latency

  The standby nodes each poll the active node periodically to draw down synchronization transactions. If the active node fails to service a poll from a standby node **within 10 seconds**, it fails over to one of the standby nodes.

Either of the network problems described above may result in the following cluster behavior:

- Multiple nodes become active as independent servers that are isolated from each other (a *split brain* state).
- Some badges may connect to one active server; other badges may connect to another active server.

The following illustration shows a simple cluster with an active node and a single standby node:
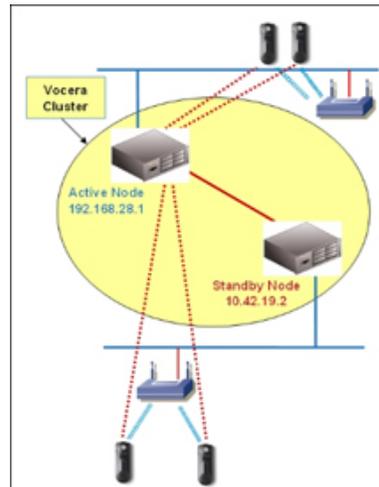
Figure 13: Simple cluster with one active and one standby server

If the network connection between the nodes is lost, the active node sends an email to indicate that it has lost contact with a standby node. The active node continues to run, and badges that have not lost a network route to it remain connected to it. Badges that cannot find this active node display "Searching for server" and begin to cycle through their list of IP addresses, looking for the active server.

The standby node notices that it has lost contact with the active node, goes into discovery mode, fails to find the active node (because the network connection is down), and comes online as an active node. This new active node sends an email stating that it has become active, and any badges that were "Searching for server" may connect to it.

This situation is known as a *split brain* because multiple cluster nodes are active, and each node is unaware of other active nodes. This split brain state is shown in the following illustration:
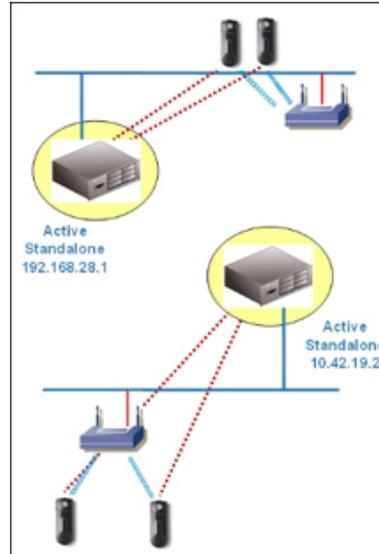
Figure 14: Simple cluster with two active servers (a "split brain" state)

Similarly, if excessive latency results in the active node failing to service a poll from a standby node within 10 seconds, the standby node enters discovery mode, the active node sends an email message indicating that it has lost contact with a standby, and one of the following situations occurs:

- If the latency is transient, the standby node may find the active node and come out of discovery mode as a standby again.

  In this situation, the standby rejoins the cluster, and the cluster does not enter a split brain state.

- If the latency is great enough, the standby node may be unable to find the active node. The standby node comes out of discovery mode as an active node, and it sends an email indicating that it has come online as an active node.

  In this situation, multiple nodes are active, and the cluster is in a split brain state.

The Self-Healing Mechanism

A *self-healing* mechanism automatically rejoins cluster nodes that are in a split brain state.

After self-healing takes effect, the node that has been active for the longest period of time remains active, and any other active nodes rejoin the cluster as standby nodes. The self-healing feature is installed automatically in Vocera 4.0 SP8 and later releases.

To support self-healing, each node keeps track of the length of time that it is active. 30 seconds after becoming active, a node notifies all other cluster nodes—active or standby—that it is active. At ongoing 30 second intervals, an active node continues to notify the other nodes of the length of time it has been active.

After the problem that caused the split brain state is resolved, the cluster nodes can communicate again. Each node then compares the length of time it has been active with the length of time other nodes have been active. The node that has been active for the longest period of time remains active; each of the other active nodes enters discovery mode and then comes online again as a standby node. Any badge that was connected to one of these new standby nodes iterates through its cluster list until it connects to the remaining active node.

Important: While the cluster is in a split brain state, the active nodes have independent databases that will get out of sync if anyone attempts to perform system maintenance. Similarly, Vocera Report Server logs and any user recordings such as messages or learned names get out of sync over time, because they are stored only on the active node to which the badge is attached. When the self-healing mechanism joins a formerly active node to the cluster as a standby, any differences on that formerly active node are lost.

Most split brain states are caused by transient network outages and are short-lived; consequently, the likelihood of independent active nodes getting out of sync is relatively small. The convenience of the self-healing feature typically outweighs the risk of losing changes made to independent active nodes. However, if you are intending to take advantage of clustering for disaster recovery purposes, you may want to disable the self-healing mechanism and rejoin cluster nodes manually.

Following is a procedure for disabling the self-healing mechanism. See Geographically Distributed Clusters on page 136 for a discussion of disaster recovery. See Manually Rejoining a Split Brain on page 134 for information about rejoining split brain nodes manually.

To disable the self-healing mechanism:

1. On each cluster node, navigate to the `\vocera\server\` directory and open the `properties.txt` file in a text editor.

2. Add the ClusterFirstSplitBrainCheckTimeMillis property and set its value to -1 as follows:

   ```
   # ClusterFirstSplitBrainCheckTimeMillis (default=30000)
   # Time between becoming active and first check
   ClusterFirstSplitBrainCheckTimeMillis = -1
   ```

3. Save the `properties.txt` file.

4. To load the updated `properties.txt` file, restart the Vocera Voice Server(s).

   a. Stop and start the standby node(s). See Stopping and Restarting the Server on page 18. The standby node(s) automatically perform a remote restore.

   b. After remote restore is completed on the standby node(s), force a failover on the active node by choosing Cluster > Failover in the Vocera Control Panel.

Troubleshooting Network Problems and Clusters

The table in this topic provides troubleshooting guidelines for interpreting the cluster email notifications you may receive in an unstable network environment.

In unstable network environments, the mail notifications that you configured as described in Cluster Email Notifications on page 130 let you know that unknown events are affecting your cluster.

Table 48: Troubleshooting network problems and clusters

Type of Email	Possible Interpretation
One mail message stating that a standby node is no longer part of the cluster.	• A planned outage on a standby node has occurred. • Transient latency has caused a standby node to enter discovery mode, and it has come back online as a standby node.
A series of mail messages stating that a standby node is no longer part of a cluster.	Excessive latency is occurring repeatedly, but it is transient enough that a standby node has not yet become active and caused a split brain to occur.
A single mail message stating that a failover has occurred.	A routine failover has occurred.
Two mail messages in quick succession, one stating that a specific IP address is no longer part of the cluster, and the other stating that a failover has occurred and the same IP address is the new active node.	A network outage or excessive latency has caused the cluster to enter a split brain state.

Type of Email	Possible Interpretation
A single mail message stating that the cluster no longer has multiple active nodes, following the two previous mail messages.	The self-healing mechanism has rejoined a split brain caused by a network outage or excessive latency.

The above table is not exhaustive. For example, a network outage may also affect the ability of a cluster node to contact the mail server, or the mail server to contact you. If you receive any cluster email-related alert, you always must investigate the health of your cluster.

Manually Rejoining a Split Brain

Before you manually rejoin a split brain, you must decide which node has the database and other files you want to preserve; this machine becomes the new active node in the rejoined cluster.

See Geographically Distributed Clusters on page 136 for additional information.

> **Important:** This procedure is necessary *only* if you have disabled the self-healing mechanism described in The Self-Healing Mechanism on page 132.

To manually rejoin a split brain:

1. Decide which of the active standalone servers has the database you want to use going forward.

   The server with the database and other files you want to keep is the *preserved* server. The other server is the *abandoned* server.

2. Make sure the network connection is back up.

3. Use the Vocera Control Panel to force a failover on the abandoned standalone server. See Using the Cluster Menu on page 19.

   The following events occur:

   - The abandoned server enters discovery mode, sees the preserved server, and comes online as a standby node for it. This new standby node then performs a remote restore from the preserved server, which is now the single active node.

   - The badges that were connected to the abandoned server find the active node and connect to it, because the active node is still in their cluster list.

   - For Vocera Report Server machines that were connected to the abandoned server, you must check the cluster list, find the active node, and connect to it.

   > **Note:** Do not use the Force Restart button on the Cluster page of the System screen to restart the abandoned server. Use the Vocera Control Panel to force all services to restart.

4. If your organization uses Staff Assignment, update the cluster list in the Staff Assignment configuration file (`app.config`) on each standby node:

   a. On each standby node, open the following file in a text editor:

      `\vocera\data\applications\staffassignment\app.config`

   b. Edit the serverIP property to include the comma-separated list of IP addresses for the Vocera Voice Server cluster. Enter numeric IP addresses using dotted-decimal notation. Do not enter domain names.

   c. Save your changes.

   > **Note:** You do not need to update the cluster list in the Staff Assignment configuration file on the active node. The serverIP property is updated automatically on the active node when someone logs into Staff Assignment.

Remote Restore Failures

If your network has an outage or experiences extreme latency during a remote restore, this synchronization operation may fail.

As described in **Synchronizing Extensive Changes** on page 129, the remote restore operation itself is fairly efficient, and it is unlikely to be the cause of such latency.

When a remote restore fails, the standby node automatically attempts to reconnect to the active node and perform the operation again. If the outage or latency was momentary, a retry is usually sufficient to allow the remote restore to complete.

If necessary, the standby node attempts to perform a remote restore a total of three times. If the remote restore fails three successive times, the standby node stops retrying and displays the following error message: "Restore from active server failed."

After you close this dialog box, the standby server becomes a standalone Vocera Voice Server, and the cluster is in a split brain state. This standalone server has an empty database, and its split brain state is more benign than the one described in **Network Problems and Clustering** on page 131 for the following reasons:

- Badge users are not affected.
- The active node remains in control of the cluster.
- The standalone server halts, preventing badges from connecting to it.

Make sure you understand and solve the network problem that caused the cluster to enter this state before starting the standalone server and attempting to rebuild the cluster. Do not start the standalone server without joining it to the cluster again, because badges that were off network when the failure occurred may return and connect to it.

To rejoin the cluster if remote restore fails three times:

1. Use the control panel to start the standalone server.
2. Open the Administration Console on the standalone server and log in.
3. Reconfigure the cluster on the standalone server. See **Add/Edit Cluster Server** on page 144.
   The standalone server enters discovery mode, finds the active node, performs a remote restore, and rejoins the cluster as a standby node.

Planned Network Outages

Following these steps will prevent failovers, a split brain, or an interruption to Vocera services.

Any network outage—even a momentary one—may result in a split brain, depending on the exact timing. When the network connection between the active node and a standby is interrupted, the standby goes into discovery mode, and one of the following situations will occur:

- If the network is available again at the time the standby node goes into discovery mode, the standby will find the active node and reconnect to it as a standby—no failover or split brain will occur. This outcome is not likely.
- If the standby node goes into discovery and cannot find the active node, it will come online as an active node, resulting in a split brain.

Prepare a cluster for a planned network outage as follows:

1. Stop the standby nodes.
2. Have the outage.
3. Restart the standby nodes.

These steps will help prevent any interuption to server, except for badges that cannot find a path to the active node because they were isolated by the outage.

If you do unintentionally create a split brain during a planned network outage, recover from it as described in **Manually Rejoining a Split Brain** on page 134.

Geographically Distributed Clusters

In addition to providing fault tolerance, the nodes in a Vocera cluster can also assist in disaster recovery if you distribute them geographically, because the database is replicated to each node in the cluster.

For example, suppose your deployment has sites in both San Diego and New York City, and you set up two cluster nodes in each of those cities. If the active node is located in San Diego, your deployment would look similar to the following illustration:
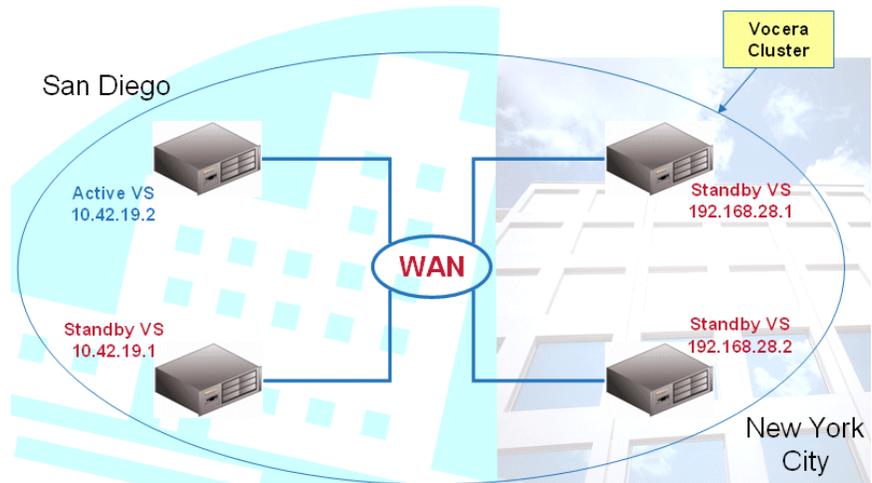
Figure 15: Geographically distributed cluster

This deployment enables disaster recovery in a variety of situations. For example, suppose an earthquake causes the WAN link between the two cities to fail, but not the cluster nodes. In this situation, the two nodes in New York form their own cluster and keep Vocera available for that city, while the two nodes in San Diego continue running as a separate cluster and provide Vocera communications for that city, as shown in the following illustration:
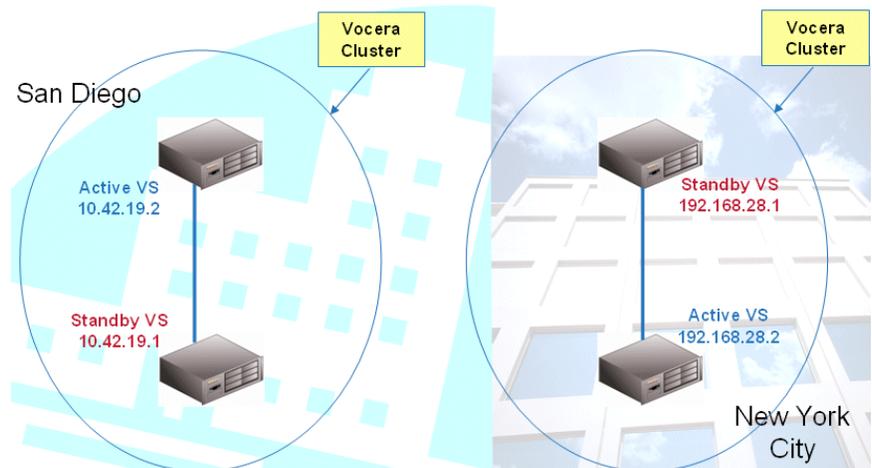
Figure 16: Geographically distributed cluster after a WAN failure

When the WAN link goes down, the two servers in New York lose contact with the active node in San Diego and go into discovery mode. One New York node emerges as an active node while the other remains in standby, and those two nodes form their own cluster. The badges in New York temporarily display searching for server, then find the active New York node.

If the original New York site has its own Vocera telephony Gateway server, that server also connects to the new active node in New York. The New York cluster starts running as an independent Vocera system within seconds. San Diego continues running and is unaffected by the outage, except it is also an independent cluster that is not connected to New York. Site-to-site calls between cities are not available until the WAN link is restored and the original cluster is re-established, but both cities continue to have Vocera service.

Because the two cities are now running independent clusters, the databases will get out of sync if anyone attempts to perform system maintenance. In addition, Vocera Report Server logs, messages, and other files will not be replicated between the two clusters. When you restore the connection between the two clusters, these changes will be lost.

In a disaster-recovery scenario, you may need to allow the independent clusters to remain separate for an indefinite period of time, increasing the likelihood that the above files will get out of sync. When the connection between the clusters is restored, these differences will be lost, as described in The Self-Healing Mechanism on page 132.

> **Tip:** If you intend to implement a geographically distributed cluster, have some form of change control in place in anticipation of a disaster. In addition, consider disabling the self-healing feature so you can manually rejoin the independent clusters after deciding how to handle any file differences.

The following table lists the system information that gets out of sync when a disaster occurs, and suggests a strategy for managing it:

Table 49: Disaster recovery strategies

What Gets Lost	Is it preventable?
Database changes.	Yes. Implement some form of change control such as one of the following: • Send a message to all system and tiered administrators telling them to avoid updating the database. Consider creating a group that revokes all tiered administrator permissions and temporarily add all the tiered administrator groups to it as members. • Record all changes you make to one system so you can update the other system with them after the independent clusters are rejoined. • Make all changes to both systems concurrently. This strategy may not be practical after a disaster and may be difficult to manage.
All user recordings (messages, learned names, and so forth)	Yes. Send a message or broadcast to Everyone, explaining what happened and warning them that their recordings will be lost.
Vocera Report Server logs.	No. The Vocera Report Server relies on statistics that are recorded during calls. While the systems are running independently, they are independently maintaining their own statistics. One of these sets of statistics will be lost when the systems are rejoined.

Manually Rejoining Independent Clusters

Learn the consideration and needed steps to rejoin independent clusters in your environment.

Before you manually rejoin independent clusters, you must decide which cluster has the database and other files you want to preserve. The active node in the cluster with the chosen database becomes the new active node in the single cluster.

> **Important:** This procedure is necessary *only* if you have disabled the self-healing mechanism described in The Self-Healing Mechanism on page 132.

To manually rejoin independent clusters after a WAN link failure:

1. Decide which of the two clusters has the database you want to use going forward.

The cluster with the database and other files you want to keep is the *preserved* cluster. The other cluster is the *abandoned* cluster.

2. Restore the WAN link.

   The two clusters continue running independently.

3. Use the Vocera Control Panel to force a failover on the active node of the abandoned cluster. See Using the Cluster Menu on page 19.

   The following events occur:

   • The standby node of the abandoned cluster enters discovery mode, sees the active node of the preserved cluster, and comes online as a standby node for it. This new standby node then performs a remote restore from the active node.

   • The formerly active node of the abandoned cluster restarts, enters discovery mode, sees the active node of the preserved cluster, and comes online as a standby node for it. This new standby node then performs a remote restore from the active node.

   • The badges that were connected to the abandoned cluster find the active node and connect to it, because the active node is still in their cluster list.

   • For Vocera Telephony Gateway server or Vocera Report Server machines that were previously connected to an abandoned cluster, you must check the cluster list, find the active node, and connect to it.

   > **Note:** Do not use the Force Restart button on the Cluster page of the System screen to restart the active node of the abandoned cluster. Use the Vocera Control Panel to force all services to restart.

A remote restore of a very large database (50,000 spoken names) across a WAN may take 20 minutes or more, depending on the actual size of the database, the speed of the WAN, the available bandwidth, and other issues outside the control of Vocera.

> **Note:** You must have a high-speed WAN link that meets the latency requirements described in the *Vocera Infrastructure Planning Guide* to support a geographically distributed cluster.

Setting up a New Cluster

This topic summarizes the procedure and steps in an initial Vocera Voice Server cluster configuration.

To set up a Vocera cluster:

1. Install all the software and hardware as follows:

   a. Perform the pre-installation tasks described in the *Vocera Voice Server Installation Guide*.

   b. Install the Vocera Voice Server on every computer that will be a member of the cluster.

      If necessary, you can also add and remove servers any time after the setup is complete.

   c. If you are using the telephony integration option, install the Vocera SIP Telephony Gateway software.

   d. If you are planning to use the Vocera Report Server, install it also.

2. On the computer(s) that will be the standby node(s), use the Vocera Control Panel to stop the Vocera Voice Server.

   > **Important:** Keep the Vocera Voice Server on the standby nodes stopped while you configure the active node. This ensures that when you start the standby nodes they will perform a remote restore from the active node because it has been running longer. Otherwise, you may unintentionally cause the active node to perform a remote restore from one of the standby nodes.

3. Prepare the Vocera Voice Server that you want to use as the initial active node as follows:

   a. On the Vocera Voice Server that you want to use as the initial active node, fully configure the database or restore an existing database.

See the *Vocera Administration Guide* for information about setting up users and groups and restoring data a backup file.

b. If you did not restore from a backup file, back up the database on the initial active node.

Although this step is not required, best practice is to do a complete backup to preserve your work in case you need to rollback to it.

c. On your configuration computer, create a `badge.properties` file that includes the IP address of every machine in your cluster in a comma-separated list.

See the *Vocera Device Configuration Guide*.

d. Copy the new `badge.properties` file to the `\vocera\config\` directory of the initial active node.

The standby nodes copy this file when they come online as cluster members. See **Data Synchronization** on page 128.

e. If you have a customized `Properties.txt` file, make sure you copy it to the `\vocera \server\` directory on every Vocera Voice Server.

f. Restart the Vocera Voice Server on the machine you want to use as the initial active node so it loads your new `Properties.txt` file and `badge.properties` file.

4. Set up clustering on the server that you want to use as the initial active node.

a. Log in to the Administration Console of the Vocera Voice Server you want to use as the initial active node.

b. Click System in the navigation bar.

c. Click the Cluster tab to display the Cluster Setup page.

The IP address of the current server appears in the server list. The Status column displays "Unsaved".

d. Check Enable Cluster.

The buttons for setting up and maintaining the cluster appear to the right of the server list.

e. Click Add Server.

The Add/Edit Cluster Server dialog box appears. Use this dialog box to add servers to a cluster.

f. Enter the IP address of a standby server and a brief description, and then do either of the following:

- If you do not need to add other nodes to the cluster, click Add to save changes, close the Add/Edit Cluster Server dialog box, and display the Cluster Setup page.

- If you need to add any other nodes to the cluster, click Add & Continue to save the information and leave the Add/Edit Cluster Server dialog box open, then add another node.

When you are finished, the server list displays the IP address of each server you added along with any descriptions you entered. The Status column for each new server displays "Unsaved".

g. Click Save Changes.

Vocera saves the information and displays the first tab of the System screen, License Info.

h. Click the Cluster tab to display the Cluster Setup page and check your work. The server list should display the following:

- The Status column for the current server displays "Active".

- The Status column for each additional server displays "Unknown".

    The cluster discovers the status of these unknown servers after you configure them for clustering and restart them.

i. Click the Log Out button at the top of the page.

The system logs you out and displays the Log In page of the Administration Console.

5. On the standby node(s), use the Vocera Control Panel to start the Vocera Voice Server.

6. Set up clustering on every other server that will be in the cluster. These additional servers will become standby nodes in the cluster.

a. Log in to the Administration Console of a server you want to use as a standby node.

b. Click System in the navigation bar.

c. Click the Cluster tab to display the Cluster Setup page.

The IP address of the current server appears in the server list. The Status column displays "Unsaved".

d. Check Enable Cluster.

The buttons for setting up and maintaining the cluster appear to the right of the server list.

e. Click Add Server.

The Add/Edit Cluster Server dialog box appears. Use this dialog box to identify the server you are using as the initial *active* server.

f. Enter the IP address of the active server and a brief description, and then click the Add button to save changes, close the Add/Edit Cluster Server dialog box, and display the Cluster Setup page.

> **Note:** You do not have to add the IP address of any other cluster servers to the list. When you restart the server you are configuring, it will download this information from the active server.

g. Click Save Changes.

Vocera saves the information and displays the first tab of the System screen, License Info.

h. Click the Cluster tab to display the Cluster Setup page. The server list should display the following:

- The Status column for the current server displays "Active".

- The Status column for the server you want to use as the initial active server displays "Unknown".

i. Click Force Restart.

A dialog box asks you to confirm restarting the server.

> **Note:** If you do not click Force Restart, within a minute the cluster's self-healing mechanism will cause the server to automatically enter discovery mode, perform a remote restore from the active server, and then come online as a standby node.

j. Click OK.

Vocera logs you out of current server's Administration Console, and the current server restarts as a standby node in the cluster. If you copied a customized `Properties.txt` file to each standby, the Vocera Voice Server loads it when it restarts.

> **Note:** You cannot log in to the Administration Console of a server after it becomes a standby node. If you attempt to log in to a standby node's Administration Console, the cluster redirects you to the Administration Console of the active node.

7. If you use the telephony integration option, open the Vocera SIP Telephony Gateway control panel and set the Server IP Address field to the IP address of the *active* Vocera Voice Server.

After you save this setting, the Vocera Voice Server populates the Server IP Address field with a comma-separated list of all cluster IP addresses. The Vocera Voice Server maintains this list if cluster nodes are added or removed.

> **Note:** You can optionally enter a comma-separated list of all cluster IP addresses manually in the Server IP Address field.

8. If you use a Vocera Report Server, open the Report Console and enter a comma-separated list of all cluster IP addresses in the **Vocera Voice Server IP Address** field.

Because the Vocera Report Server does not communicate continually with the Vocera Voice Server, you must enter every cluster IP address. The Vocera Report Server does not maintain this list of addresses.

9. Check your work.

Log in to the Administration Console of the active Vocera Voice Server. Make sure each server shows up in the list on the Cluster Setup page with the proper status of "active" or "standby".

Fail over cluster control several times, until you confirm that the cluster behaves as you expect. See the Vocera Voice Server Installation Guide.

Adding a Node to an Existing Cluster

You can add an additional node to an existing cluster at any time without causing the active server to fail over.

Vocera supports up to four servers in a cluster.

To add a new server to an existing cluster:

1. On the new server that you want to add to the cluster, use the Vocera Control Panel to stop the Vocera Voice Server.

   Important: Keep the Vocera Voice Server on the new standby node stopped while you configure the active node. This ensures that when you start the standby node it will perform a remote restore from the active node because it has been running longer. Otherwise, you may unintentionally cause the active node to perform a remote restore from the new standby node.

2. Configure the active node to recognize the new server.
   a. Log in to the Administration Console of the active node.
   b. Click System in the navigation bar.
   c. Click the Cluster tab to display the Cluster Setup page.
   d. Click Add Server.
      The Add/Edit Cluster Server dialog box appears. Use this dialog box to add servers to a cluster.
   e. Enter the IP address of a standby server and a brief description.
   f. Click Add to save changes, close the Add/Edit Cluster Server dialog box, and display the Cluster Setup page.
      When you are finished, the Status column for the new server displays "Unsaved".
   g. Click Save Changes.
      Vocera saves the information and displays the first tab of the System screen, License Info.
   h. Click the Log Out button at the top of the page.
      The system logs you out and displays the Log In page of the Administration Console.

3. On the new server that you want to add to the cluster, use the Vocera Control Panel to start the Vocera Voice Server.

4. Configure the new server to recognize the active node.
   a. Log in to the Administration Console of a server you want to use as a standby node.
   b. Click System in the navigation bar.
   c. Click the Cluster tab to display the Cluster Setup page.
      The IP address of the current server appears in the server list. The Status column displays "Unsaved".
   d. Check Enable Cluster.
      The buttons for setting up and maintaining the cluster appear to the right of the server list.
   e. Click Add Server.
      The Add/Edit Cluster Server dialog box appears. Use this dialog box to identify the server you are using as the *active* server.
   f. Enter the IP address of the active server and a brief description, and then click the Add button to save changes, close the Add/Edit Cluster Server dialog box, and display the Cluster Setup page.

> **Note:** You do not have to add the IP address of any other cluster servers to the list. When you restart the server you are configuring, it will download this information from the active server.

g. Click Save Changes.

Vocera saves the information and displays the first tab of the System screen, License Info.

h. Click the Cluster tab to display the Cluster Setup page.

i. Click Force Restart.

A dialog box asks you to confirm restarting the server.

> **Note:** If you do not click Force Restart, within a minute the cluster's self-healing mechanism will cause the server to automatically enter discovery mode, perform a remote restore from the active server, and then come online as a standby node.

j. Click OK.

Vocera logs you out of current server's Administration Console, and the current server restarts as a standby node in the cluster.

5. If your organization uses Staff Assignment, update the cluster list in the Staff Assignment configuration file (`app.config`) on each standby node:

a. On each standby node, open the following file in a text editor:

`\vocera\data\applications\staffassignment\app.config`

b. Edit the serverIP property to include the comma-separated list of IP addresses for the Vocera Voice Server cluster. Enter numeric IP addresses using dotted-decimal notation. Do not enter domain names.

c. Save your changes.

> **Note:** You do not need to update the cluster list in the Staff Assignment configuration file on the active node. The serverIP property is updated automatically on the active node when someone logs into Staff Assignment.

6. Check your work.

a. Log in to the Administration Console of the active Vocera Voice Server. Make sure each server shows up in the list on the Cluster Setup page with the proper status of "active" or "standby".

b. Fail over cluster control several times, until you confirm that the cluster behaves as you expect. See the Vocera Voice Server Installation Guide.

Editing the Information for a Clustered Node

You can edit information for any of the nodes in your cluster at any time where the result you see depends upon the type of edit you performed.

The following table lists what happens in a cluster when you make various changes.

Table 50: Editing cluster node information

If you change:	The following occurs:
The IP address of one Vocera Voice Server to another Vocera Voice Server's IP address.	This situation is equivalent to deleting an existing server and adding a new one: • The server whose IP address you changed is removed from the cluster. The removed server becomes active as a standalone server. • The server whose IP address you entered is added to the list of servers in the cluster. You must configure clustering in this new server and restart it. See Adding a Node to an Existing Cluster on page 141.
An invalid Vocera Voice Server IP address to a valid Vocera Voice Server IP address.	This situation is equivalent to adding a new server to a cluster. The server whose IP address you entered is added to the list of servers in the cluster. You must configure clustering in this new server and restart it. See Adding a Node to an Existing Cluster on page 141.
A valid Vocera Voice Server IP address to an invalid Vocera Voice Server IP address.	The server appears in the list of cluster servers, but it is not actually added to the cluster.

If you change:	The following occurs:
The description of a Vocera Voice Server.	The new description appears in the list of cluster servers.

To edit the information for a clustered node:

1. Click System in the navigation bar.
2. Click the Cluster tab to display the Cluster Setup page.
3. In the list, choose the server you want to edit.
4. Click Edit Server.
   The Add/Edit Server dialog box appears.
5. Modify the information for the server as described in **Add/Edit Cluster Server** on page 144.
6. Click Add to save changes.
   The Edit Cluster Server dialog box closes, and the Cluster Setup page is displayed again. The new information appears in the list.
7. Click Save Changes.
   Vocera saves the information on the Cluster Setup page.

Removing a Server from a Cluster

You can remove a standby server from a cluster at any time. You cannot remove the active server unless you first fail over control to another node.

When you remove a standby server from a cluster, it becomes active as a standalone server. This standalone server does not interfere with the cluster, because it has a different IP address than the active server, and the active server knows that it is no longer a cluster member if a failover occurs.

To remove a server from the cluster:

1. Click System in the navigation bar.
2. Click the Cluster tab to display the Cluster Setup page.
3. Select the server you want to remove in the list. The server appears highlighted.
4. Click Delete Server.
   A dialog box asks you to confirm the deletion.
5. Click OK.
   Vocera removes the highlighted server from the cluster list.
6. Click Save Changes to save the information on the Cluster Setup page.
   Vocera removes the server from the cluster. The removed server becomes active as a standalone server.
7. If your organization uses Staff Assignment, update the cluster list in the Staff Assignment configuration file (`app.config`) on each standby node:
   a. On each standby node, open the following file in a text editor:
      `\vocera\data\applications\staffassignment\app.config`
   b. Edit the serverIP property to include the comma-separated list of IP addresses for the Vocera Voice Server cluster. Enter numeric IP addresses using dotted-decimal notation. Do not enter domain names.
   c. Save your changes.

   Note: You do not need to update the cluster list in the Staff Assignment configuration file on the active node. The serverIP property is updated automatically on the active node when someone logs into Staff Assignment.

Changing the Failover Sequence

Learn the steps to changing how failovers are handled in a cluster.

A standby server pings the active server every 10 seconds to make sure it is still active. When a standby server notices that the active server has failed, it goes into a "discovery" mode to find out the status of other servers in the cluster. If all other servers are still in standby, the server that entered discovery mode takes control of the cluster.

On some occasions, multiple standby servers may enter discovery mode at the same time. In this situation, the order in which servers are listed on the Cluster Setup page determines the order in which they will take control when failovers occur.

To change the failover sequence of servers in a cluster:

1. Click System in the navigation bar.
2. Click the Cluster tab to display the Cluster Setup page.
3. Choose the server you want to reorder in the list.
4. Click Move Up or Move Down to change the sequence of servers in the list.
5. Reorder any other servers, then click Save Changes.
   Vocera saves the new sequence on the Cluster Setup page.

Failing Over and Restarting Clustered Servers

Learn how to kickoff a restart in a cluster.

You can use the Cluster Setup page of the Administration Console to restart the current Vocera Voice Server (the server you are browsing with the Administration Console):

- If the current Vocera Voice Server is *active*, it restarts and the cluster fails over control to one of the standby servers.
- If the current Vocera Voice Server was just added to the list of cluster members, it restarts and joins the cluster.

You can use the Cluster Setup page of the Administration Console to force a failover of the active server. If you have just entered a server in the list of clustered nodes, the Cluster Setup page lets you restart it to add it to the cluster.

To fail over or restart a server:

1. Click System in the navigation bar.
2. Click the Cluster tab to display the Cluster Setup page.
3. Click Force Restart.
   A dialog box asks you to confirm.
4. Click OK.
   Vocera logs you out of the Administration Console, and either of the following situations occurs:
   - If you were in the Administration Console of the active server, it fails over control to one of the standby servers.
   - If you were using the Administration Console of a server that was just added to the list of clustered nodes, it restarts as a standby node in the cluster.
   The server performs a fast restart. It does not perform a full restart of all Vocera-related services. You must use the Failover command in the Cluster menu of the Vocera Control Panel to perform a full restart.

Add/Edit Cluster Server

The Add/Edit Cluster Server dialog box lets you add a server to a cluster or edit the identifying information for an existing server in a cluster.

Table 51: Cluster server fields

Field	Maximum Length	Description
IP Address	15	Enter the numeric IP address of the machine. Note: You must use the numeric IP address, not the DNS name.
Description	100	Optionally provide a brief description to help you identify the machine.

Updating Property Files for a Cluster

Learn about the property files in the Vocera Voice Server environment and how to update them.

The following files define properties for the Vocera Voice Server, and the Vocera SIP Telephony Gateway.

- `\vocera\server\properties.txt`
- `\vocera\config\badge.properties.txt`
- `\vocera\telephony\vgw\vgwproperties.txt`

These files provide default values that are appropriate for most installations. However, you may choose to edit these files to specify specialized behavior for your Vocera system. This is an optional configuration task that can be performed any time after installation.

To update the property files:

1. Use a text editor to modify the property files for each Vocera Voice Server node.

   Note: If you are using the same property file on each Vocera Voice Server, you can edit one of the property files and then copy it to the other server(s).

2. To load the updated `properties.txt` file, restart the Vocera Voice Server(s).
   a. Stop and start the standby node(s). See **Stopping and Restarting the Server** on page 18. The standby node(s) automatically perform a remote restore.
   b. After remote restore is completed on the standby node(s), force a failover on the active node by choosing Cluster > Failover in the Vocera Control Panel.

3. To load the updated `vgwproperties.txt`, restart the Vocera Telephony Gateway server(s). If you have multiple telephony servers:
   a. Stop and start one server at a time.
   b. Wait until the telephony server has started before stopping and then starting the next telephony server in the array until all telephony servers have been restarted.

Configuring Active Directory Authentication

The Active Directory page of the Administration Console configures Active Directory authentication, which lets Vocera users log in using their network credentials.

The following checklist provides an overview of the Active Directory configuration steps:

☐	Make sure your Active Directory server meets requirements. See About Active Directory Authentication on page 147.
☐	Optionally, enable SSL on Active Directory. If you choose to not enable SSL on Active Directory, user credentials passed between Active Directory and the Vocera Voice Server are not encrypted. If you enable SSL on Active Directory and are using self-signed certificates, you need to add the SSL certificate for each Active Directory server to the Vocera Voice Server Java keystore. See Managing Active Directory Certificates on page 155.
☐	Add an Active Directory configuration to the Active Directory Configuration list, or edit an existing Active Directory configuration. See Adding or Editing an Active Directory Configuration on page 150.
☐	Test the connection for an Active Directory configuration to make sure it works. See Testing an Active Directory Connection on page 152.
☐	Establish a persistent connection from the Vocera Voice Server to an Active Directory configuration. See Connecting to and Disconnecting from an Active Directory Configuration on page 153.
☐	Test whether a user can use an Active Directory connection to log into Vocera Voice Server applications. See Testing a User Login on page 154.
☐	If the test login is successful, enable the Active Directory configuration to turn on Active Directory authentication for the Vocera

		Administration Console, User Console, and Staff Assignment clients. See **Enabling and Disabling an Active Directory Configuration** on page 155.
	☐	If you have multiple Active Directory domains, repeat these steps to add other Active Directory configurations as needed.

About Active Directory Authentication

Active Directory is not used for authorization of Vocera users since its handled by Vocera permission groups.

Active Directory is Microsoft's LDAP directory service for Windows domain networks. It is included with most versions of Microsoft Windows Server. The Active Directory domain controller performs many functions, such as authenticating and authorizing all users and computers in a Windows domain type network. However, Vocera uses Active Directory only to authenticate users using the central Active Directory database.

If you configure the Vocera Voice Server to use Active Directory authentication, users can log into Vocera Voice clients (such as the Administration Console or Staff Assignment) with their current network credentials. All user passwords reside in Active Directory rather than in the Vocera Voice Server database, simplifying administration.

You must configure both the Vocera Voice Server and the Active Directory server for Active Directory authentication to work correctly. Depending on how your Vocera user accounts have been set up, you may need to map an Active Directory login attribute to use for authentication. This login attribute binds the Active Directory credentials to a Vocera user account.

Preparing for Active Directory Authentication:

1. Make sure your Active Directory server is the correct version.
   See **Supported Versions of Active Directory** on page 147.
2. If SSL is enabled on Active Directory, obtain the SSL CA certificate from the Active Directory and copy it to the Vocera Voice Server machine.
   See **Managing Active Directory Certificates** on page 155.
3. Make sure your Active Directory server has a service account with read access to the directory. Obtain the user ID of this account and the password.
4. Identify the login map field, the Active Directory field that binds Active Directory credentials to a Vocera user account. You need this field name to configure Active Directory authentication in the Vocera Administration Console.
   See **Login Map Field Requirements** on page 148.

   > **Important:** Make sure that all Vocera users have their Vocera user ID specified in the login map field. Otherwise, they won't be able to log into the Vocera Administration Console, User Console, or Staff Assignment clients.

Supported Versions of Active Directory

This topics lists the suported Windows versions of Active Directory.

Active Directory authentication is supported on the following versions of Active Directory:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

User ID and Password Limits

The maximum lengths on user IDs and passwords are different depending on which authentication type you choose.

Table 52: User ID and Password maximum lengths

Vocera authentication	Max Length	Active Directory authentication	Max Length
User ID	50	userPrincipalName	249 for Staff Assignment; 250 for Administration Console and User Console.
		sAMAccountName	20
Password	25	Password	127

Login Map Field Requirements

To use Active Directory authentication for Vocera clients, your IT department must identify the login map field, the Active Directory attribute that binds Active Directory credentials to a Vocera user account.

The login map field for Vocera must meet the following requirements:

- The field must uniquely identify a Vocera user. Duplicate values are not allowed.
- The field must contain only letters, digits, spaces, periods (.), underscores (_), or dashes (-). No other characters are allowed.
- The field is limited to 50 characters.
- The field must not begin or end with a space.

Quite often, user IDs in the Vocera database match the sAMAccountName attribute in Active Directory. However, sAMAccountName is limited to 20 characters. If your Vocera user IDs are longer than 20 characters, you need to use an attribute other than sAMAccountName for the login map field.

To verify that the login map field is mapped appropriately, it may be necessary to export user IDs from the Vocera system to a CSV file to compare them with the login map field in Active Directory. If any Vocera user IDs don't match, you may need to update them. For details about exporting Vocera users, see **Exporting Data to a CSV File** on page 166.

Using a Global Catalog Server

For faster authentication, you can use a global catalog server for authentication. A global catalog server is an Active Directory domain controller that has been granted the Global Catalog (GC) role.

The global catalog is a partial representation of all objects from every domain within the Active Directory forest. The Vocera Voice Server can search Active Directory, but it does not need to refer to specific domain controllers that store the requested user data.

The default global catalog SSL port is 3269. If you decide to use a global catalog server, firewall rules must allow inbound traffic to port 3269 on the domain controller.

If you have only one domain, Microsoft recommends that you configure all domain controllers as global catalog servers.

Vocera Administrator Account Authentication

Vocera provides a built-in administrator account with the user ID Administrator. Regardless if Active Directory authentication is enabled, the Administrator account does not use Active Directory credentials to log in.

The default Administrator password is admin, but you can change it. See **Setting Passwords** on page 108.

Windows Domain Password Policies

A secure enterprise network requires all users to use strong passwords, which have at least eight characters and include a combination of letters, numbers, and symbols.

Strong passwords that are changed regularly help prevent attackers from guessing passwords and compromising users accounts.

Windows Server 2008 Active Directory domains support fine-grained password policies, which let you define different password and account lockout policies for different groups of users in a domain. In Windows Server 2003 Active Directory domains, only one password policy and account lockout policy can be applied to all users in the domain.

Once Active Directory authentication is enabled, the Active Directory password policy takes effect for all users logging into the Administration Console, User Console, and Staff Assignment applications.

There are several password policy settings that control the complexity and lifetime of Windows domain passwords:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Passwords must meet complexity requirements
- Store password using reversible encryption

For more information about Windows domain passwords, see the following Microsoft TechNet article: **Passwords Technical Overview**.

Coordinating with Your IT Department

Learn the information you must provide to the IT group in order to add Active Directory.

To add an Active Directory configuration into the Vocera Administration Console, gather the following information from your IT department:

- The Active Directory domain
- The list of primary and secondary Active Directory servers for each domain controller
- The Active Directory service account and password used to connect to the server
- Whether the domain controller is a Global Catalog Server
- Optionally, a search base to speed authentication
- The Active Directory field used to map an Active Directory account to a Vocera user ID

Using the Active Directory Page

When you click Active Directory in the navigation bar, the Active Directory page appears. The main part of the page is the Active Directory Configuration table, which lists all Active Directory configurations you have added.

If your organization has multiple Active Directory domains, you can add multiple configurations. Otherwise, only one configuration may be needed. At the right of the table and below it are several buttons to manage configurations.

The order of Active Directory configurations also determines the order that enabled Active Directory configurations are listed on the login page of the Vocera Administration Console, User Console, and Staff Assignment clients.

Active Directory Configuration Table

The Active Directory Configuration table has the following fields:

Table 53: Active Directory Configuration table fields

Field	Description
Name	The name of the Active Directory configuration. This name is used to identify the Active Directory server when users log in.
Domain	The domain name of the Active Directory server.
Connected Server	The currently connected Active Directory server for the configuration. If the configuration was never connected, or someone disconnected the configuration, the field is blank. If the configuration was connected, but the Vocera Voice Server is unable to make a connection, the field displays, "Could not connect to the server."
Enabled	Whether the Active Directory configuration is currently enabled. **Important:** If any one of the Active Directory configurations is enabled, Active Directory authentication is turned on and users of the Administration Console, User Console, and Staff Assignment clients must log in using their Active Directory credentials.

Active Directory Configuration Buttons

The Active Directory page has the following buttons to manage configurations:

Table 54: Active Directory Configuration buttons

Button	Description
Connect	Establishes a persistent connection to the selected Active Directory configuration from the Vocera Voice Server.
Disconnect	Disconnects the selected Active Directory configuration from the Vocera Voice Server.
Test Login	Tests whether a user can use the selected Active Directory connection to log into Vocera Voice Server applications.
Enable	Makes the connection to the selected Active Directory configuration active. The name of the configuration appears on the Login page for the Vocera Administration Console, User Console, and Staff Assignment applications.
Disable	Disables the connection to the selected Active Directory configuration. The name of the configuration is removed from the Login page for the Vocera Administration Console, User Console, and Staff Assignment applications.
Add	Adds a new Active Directory configuration.
Edit	Edits an existing Active Directory configuration.
Delete	Deletes the selected Active Directory configuration. If the configuration was connected, the connection is ended.
Refresh	Refreshes the Active Directory Configuration table with the latest information.

Adding or Editing an Active Directory Configuration

Use the Add/Edit Active Directory Configuration dialog box to add or edit the configuration for an Active Directory server.

After you save a configuration, you can enable the configuration to use for authentication. If your organization has multiple Active Directory domains, you can add multiple configurations.

To add or edit an Active Directory configuration:

1. Click Active Directory in the navigation bar.

2. Click Add to add a new Active Directory configuration, or choose an Active Directory name from the list and click Edit to edit an existing configuration.

The Add/Edit Active Directory Configuration dialog opens. Add or edit data as appropriate.

Table 55: Add/Edit Active Directory Configuration fields

Field	Maximum Length	Description
Name	50	Enter the name for this Active Directory configuration. This name is used to identify the Active Directory server when users log in, so give it a name that users will recognize, such as the name of a site, organization, or division. The name must be unique; it cannot be the name of an existing Active Directory configuration.
Primary Servers	255	Enter the comma-separated list of Active Directory server IP addresses or DNS names. **Important:** You can specify a total of seven servers between the Primary Servers and Secondary Servers lists.
Secondary Servers	255	Optionally, enter the comma-separated list of secondary Active Directory server IP addresses or DNS names. The secondary servers are used only if the Vocera Voice Server is unable to connect to any of the primary Active Directory servers. The secondary servers could be Active Directory servers installed at a remote site for redundancy purposes.
SSL	n/a	If the Active Directory uses LDAP over SSL (LDAPS), check this box. If you check the SSL box, you must install the Active Directory certificate on each Vocera Voice Server.
Port	5	Type the TCP port used by Active Directory. The valid range is 1 to 65535. The default is port 636. If your Active Directory server is a global catalog server, you can change the port to 3269, the global catalog SSL port, to speed up authentication. Here is a list of default Active Directory ports: - LDAP—389 - LDAP SSL—636 - LDAP Global Catalog—3268 - LDAP Global Catalog SSL—3269
AD Service Account ID	50	Enter the user ID for an Active Directory service account. This service account should have read access to Active Directory.
Domain	50	Enter the fully qualified domain name (FQDN) of the Active Directory server.
AD Service Account Password	30	Enter the password of the Active Directory service account.
Re-enter Password	30	Re-type the same password you entered in the AD Service Account Password field.

Field	Maximum Length	Description
Search Base	50	Optionally, type the location in which to start searching in the Active Directory hierarchical structure for user account entries. By specifying a search base, you can make authentication faster by not searching the entire Active Directory. A search base comprises multiple objects separated by commas. These objects can include a common name (cn), organizational unit (ou), organization (o), country (c), and domain (dc). For example, to search the Support container in the vocera.com domain, specify the following search context: `ou=support,dc=vocera,dc=com` **Note:** The search base is case-insensitive. If you don't specify a search base, the entire Active Directory domain is used as the search base.
Login Map Field	50	Enter the Active Directory user attribute used to map the Active Directory account to a Vocera user ID. For example, Active Directory may have an attribute for the employee ID that maps to Vocera user IDs. Make sure you enter the Ldap-Display-Name of the attribute, not its common name (cn). If you're not sure of the Ldap-Display-Name, check with your Active Directory administrator. **Note:** The field name is case-sensitive.

3. After completing the Active Directory configuration, do either of the following:

- Click Save to save changes and close the dialog box.
- Click Save & Continue to save changes and clear the Add/Edit Active Directory Configuration dialog box, letting you add information for another Active Directory configuration.
- Click Test Connection to test whether you can connect successfully to the Active Directory servers, both primary and secondary, using the current settings.

Testing an Active Directory Connection

Learn about testing your Active Directory configuration.

In the Add/Edit Active Directory Configuration window, you can click the Test Connection button to test whether you can:

- Establish a connection with each Active Directory server (both primary and secondary).
- If SSL is enabled on Active Directory, verify the SSL certificate.
- Authenticate the service account with the Active Directory server.
- Verify the Search Base.

The Active Directory connection is set up only temporarily for test purposes. Once the test is completed, the connection is terminated.

Note: The Login Map Field is not verified when you test the connection. That field is verified when you test logging into an Active Directory configuration. See **Testing a User Login** on page 154.

When you click Test Connection, the Active Directory Test Connect Results window appears, showing connection results for each Active Directory server. The window provides diagnostic information to help you troubleshoot connection problems.

At the top of the window, the following three fields appear:

- Name—name of the configuration
- Domain—domain name of the Active Directory server
- Service Account ID—user ID for an Active Directory service account

Below these three fields, a table provides information about the connection to each Active Directory server:

Table 56: Test Connection Results fields

Field	Description
Server Addresses	Indicates whether the Active Directory server is Primary or Secondary, and displays the server's IP address and DNS name.
Establish Connection	Displays whether an LDAP connection could be established with the Active Directory server and the time (in milliseconds) it took to complete the connection.
Verify Certificate	Displays whether the Active Directory root certificate was verified successfully. If there was a problem, the full error appears in the Error Detail column.
Authenticate Service Account	Displays whether the service account could be authenticated and the time (in milliseconds) it took to complete authentication.
Verify Search Base	Displays whether the Search Base was verified successfully. If the Search Base is not specified, the entire Active Directory domain is used as the search base.
Error Summary	Displays any errors found in the connection parameters or service account credentials. This field helps identify quickly which part of the configuration has been entered incorrectly. If there are no errors, this field is empty.
Error Detail	Displays detailed diagnostic information about an error. If there are no errors, this field is empty.

Evaluating Connection Times

Pay attention to the time it takes to establish a connection for each of the Active Directory servers. Servers that take the longest time to connect should be selected as Secondary Servers.

Showing Connection Results in Printable Format

To view the Active Directory Test Connection Results window in printable format, click the Printable Format button.

Connecting to and Disconnecting from an Active Directory Configuration

Once you set up an Active Directory configuration, you can establish a persistent connection to it from the Vocera Voice Server.

The connection will be maintained as long as a Vocera Voice Server is active. If you restart the Vocera Voice Server machine, the connection will resume when the server comes online. By default, the Vocera Voice Server checks the status of the connection every minute. If a connection fails, the servers attempts to connect to another Active Directory server in the list of Primary Servers first, and then Secondary Servers.

To connect to an Active Directory configuration:

1. In the Active Directory Configuration list, select a configuration that is not connected. The value in its status field must be "Not Connected."
2. Click Connect.
3. When prompted, click OK.

   The Vocera Voice Server attempts to establish a connection to the Active Directory. If the connection is successful, the Status field changes to "Connected" and shows the IP address of the connected Active Directory server.

To disconnect from an Active Directory configuration:

1. In the Active Directory Configuration list, select an Active Directory configuration that is connected. The value in its status field must be "Connected."
2. Click Disconnect.
3. When prompted, click OK.

Refreshing the Status of an Active Directory Configuration

When you establish a persistent connection for an Active Directory configuration by clicking Connect on the Active Directory screen, the server does not update the connection status continuously.

Consequently, the page may indicate that an Active Directory server is connected (or disconnected) when it is not.

To refresh the page with the latest connection information, click Refresh.

Monitoring an Active Directory Connection

After you establish a persistent connection for an Active Directory configuration, don't enable the Active Directory configuration immediately. Instead, monitor the connection on the Active Directory page of the Administration Console for several hours to ensure it is reliable.

To get the latest status, refresh the page. After you confirm that the Active Directory connection is reliable and functioning properly, you are ready to enable it.

If there is a problem with the connection, the Vocera Voice Server sends an email alert. For more information, see Troubleshooting Active Directory Connectivity on page 157.

Testing a User Login

After you enable an Active Directory configuration, you are ready to test whether a user can use the Active Directory connection to log into Vocera Voice Server applications such as the Administration Console, User Console, and Staff Assignment.

To login successfully, the specified Login Map Field on the Active Directory must have a valid Vocera Voice Server user ID.

To test a user login using Active Directory authentication:

1. In the Active Directory Configuration list, select a configuration with an active connection. The value in its Connection Status field must be "Connected."
2. Click Test Login.
   The Test Active Directory User Login dialog box appears.

   > **Note:** If the Connection Status of the Active Directory configuration is "Not connected," an error message appears when you click Test Login.

3. Enter the Active Directory user and password, and then click Test.
4. A dialog box displays information about whether the login was successful. Click Close.
5. Click Close to close the Test Active Directory Login dialog box.

Test Active Directory User Login Error Messages

When you click Test Login, the user is either successfully authenticated or not.

If authentication fails, one of the following error messages appears:

Table 57: Test Active Directory User Login Error Messages

Error message	Description
Invalid Login Map Field.	The specified Login Map Field does not exist in Active Directory.

Error message	Description
Invalid <LoginMapFieldName> value in Active Directory; user not found on the Vocera Voice Server.	The value in the Login Map Field does not correspond to a user ID in the Vocera Voice Server.
Invalid password.	The password is incorrect for the specified user.
No such user.	The specified user does not exist in Active Directory, or it is not found in the specified Search Base.
Password is required.	The User Password field cannot be blank.
User ID is required.	The User ID field cannot be blank.

Deleting an Active Directory Configuration

If you don't need an Active Directory configuration anymore, you can remove it from the Active Directory Configuration list.

To delete an Active Directory configuration:

1. In the Active Directory Configuration list, select a configuration.
2. Click Delete.
   A confirmation dialog box appears.
3. Click OK.

Enabling and Disabling an Active Directory Configuration

By default, Active Directory configurations are not enabled when you create them.

When you are ready to make the connection to the Active Directory server active, select one in the Active Directory Configuration list, and then click Enable.

To disable a configuration, select it in the list, and click Disable.

> **Important:** If any one of the Active Directory configurations is enabled, Active Directory authentication is turned on. Subsequently, all Vocera users need to log into the Vocera Administration Console, User Console, and Staff Assignment clients using their Active Directory credentials.

Managing Active Directory Certificates

If you enable SSL on Active Directory servers, user credentials passed between Active Directory and the Vocera Voice Server are always encrypted.

When SSL is enabled, the Active Directory server requires an SSL certificate. How you manage certificates depends on whether you use self-signed certificates or trusted certificate authority (CA) certificates:

- **Self-signed certificates**—Export the root SSL certificate from each Active Directory server and then add it to the Java keystore on each Vocera Voice Server machine.
- **Trusted CA certificates**—The root certificate (such as one from Go Daddy or VeriSign) likely already resides in the Java keystore on the Vocera Voice Server and you don't need to export it. However, if the CA certificate for your Active Directory server is part of a certificate chain, then you must add each *intermediate* CA certificate in the hierarchy to the Java keystore on each Vocera Voice Server machine.

Configuring Active Directory for SSL Access

Review documentation related to Active Directory from Microsoft.

See the following Microsoft articles for instructions on how to enable SSL access for Active Directory:

- LDAP over SSL (LDAPS) Certificate[1]
- How to enable LDAP over SSL with a third-party certification authority[2]

Verifying that SSL Is Enabled on Active Directory

Once you have enabled SSL on Active Directory, you can verify that the connection to Active Directory is using SSL and is encrypted.

To verify that SSL has been enabled on the Active Directory server:

1. Start the Active Directory Administration Tool (`Ldp.exe`). For more information, see the following links:
   - Ldp Overview[3]
   - Remote Server Administration Tools (RSAT) for Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012[4]
2. Choose Connection > Connect.
3. Type the name of the Active Directory domain controller to which you want to connect.
4. Type `636` as the port number, and make sure the SSL checkbox is checked.
5. Click OK.

Exporting the Active Directory SSL Certificate

When you install Active Directory Certificate Services and create a root CA certificate for the Active Directory server, the certificate is automatically created at the root of the `C:\` drive.

For example: `c:\ad2008.ad01.vocera.com_ad01.crt`.

There are two ways you can export the CA certificate:

- Use the `certutil` command-line utility.
- Request the root CA certificate from the CA Web Enrollment Site.

Using the Certutil Utility to Export a CA Certificate

Learn the cerutil command for exporting certificates.

To export a CA certificate from the Active Directory server, you can use the certutil command-line utility:

```
certutil -ca.cert CACertFile
```

where *CACertFile* is the full path and filename of the CA certificate (for example, `c:\certnew.cer`).

Requesting the Root CA Certificate from the Web Enrollment Site

You can request the root CA certificate for the Active Directory server by going to the CA web enrollment site for the server.

To request the root CA certificate from the web enrollment site:

---

[1] http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx"

[2] http://support.microsoft.com/kb/321051

[3] http://technet.microsoft.com/en-us/library/cc772839%28WS.10%29.aspx

[4] http://social.technet.microsoft.com/wiki/contents/articles/2202.remote-server-administration-tools-rsat-for-windows-vista-windows-7-windows-8-windows-server-2008-windows-server-2008-r2-and-windows-server-2012-dsforum2wiki.aspx

1. Open a browser, and log into Root Certification Authority Web Enrollment Site for the Active Directory server. It is usually available at one of the following links:

   `http://`*`ip_address`*`/certsrv`

   or

   `http://`*`fqdn`*`/certsrv`

   where

   - *ip_address* is the root CA server IP address
   - *fqdn* is the fully-qualified domain name of the root CA server

2. Click the Download a CA certificate, certificate chain, or CRL link.
3. Click Download CA certificate.
4. Save the file `certnew.cer` to a local drive.

Adding the Active Directory SSL Certificate to the Vocera Voice Server Java Keystore

After you export the CA certificate for the Active Directory server, you must add it to the Java keystore on each Vocera Voice Server machine.

To add the Active Directory SSL certificate to the Java keystore on the Vocera Voice Server machine:

1. Copy the CA certificate from the Active Directory server to the Vocera Voice Server machine. For example, copy it to the root of the `C:` drive on the Vocera Voice Server machine.
2. Open a Command Prompt window.
3. Change to the `%VOCERA_DRIVE%\vocera\server` folder:

   `cd %VOCERA_DRIVE%\vocera\server`

4. Run the following command:

   `importcert.bat `*`Alias Certpath`*

   where

   - *Alias* is the IP address of the Active Directory server
   - *CertPath* is the full path and file name of the CA certificate (for example, `c:\certnew.cer`)

   Important: If you uninstall and then reinstall the Vocera Voice Server, you must add the Active Directory SSL certificate to the Java keystore again.

Troubleshooting Active Directory Connectivity

The Vocera Voice Server sends an email alert whenever there is a problem with the connection of one of the Active Directory configurations (whether the connection is enabled or not). The following table describes the Active Directory email alerts/warnings:

Table 58: Active Directory alerts and warnings

Alert/Warning	Description	Corrective action needed
Active directory connection for < *Active Directory Configuration Name*> failed.	The Vocera Voice Server connection to the Active Directory configuration failed, whether one or multiple servers are specified, including primary and secondary servers. By default, a new alert is sent every 30 minutes until the Active Directory connection is restored.	Work with IT to ensure that all Active Directory domain controllers are running. Once Active Directory domain controllers are running, the Vocera Voice Server will automatically connect to one of them. You don't need to disable and then enable the Active Directory configuration in the Administration Console.

Alert/Warning	Description	Corrective action needed
All primary Active Directory domain controllers for connection < *Active Directory Configuration Name*> are down. Now connected to *<Secondary Active Directory IP Address>* (Secondary server).	The Vocera Voice Server connection to the Active Directory has switched from a primary server to a secondary server. By default, another email alert is sent every day until the connection to a primary server is successful.	Work with IT to ensure that a primary Active Directory domain controller is running and is accessible over the network. Once a primary Active Directory domain controller is running, do this: 1. Disconnect the Active Directory configuration. If the configuration is currently enabled, disconnecting it also disables it. See **Connecting to and Disconnecting from an Active Directory Configuration** on page 153. 2. Connect the Active Directory configuration. 3. If the Active Directory configuration was previously enabled, enable it again. See **Enabling and Disabling an Active Directory Configuration** on page 155.

Handling Active Directory Authentication Response Timeouts

If the Active Directory does not respond to an authentication request or is unable to find a user in a specified Search Base within one second, authentication times out and the login fails.

The error message the user sees is, "Timeout error." If users complain of Active Directory response timeouts, Vocera recommends that you improve the speed of authentication by configuring an Active Directory domain controller as a global catalog server. See **Using a Global Catalog Server** on page 148.

Turning Off Active Directory Authentication

Learn the steps to disable Active Directory using the Administration Console.

To turn off Active Directory authentication:

1. Log into the Administration Console using the built-in Administrator user ID. The default password for the Administrator account is admin, but your organization may have changed it.
2. Click Active Directory in the navigation bar.
3. Disable all Active Directory configurations:
    a. Select an Active Directory configuration that is enabled.
    b. Click Disable to disable it.
    c. Click OK.
    d. Repeat for all other enabled Active Directory configurations until all are disabled.
4. Notify Vocera users that they must now log into Administration Console, User Console, and Staff Assignment using Vocera credentials.

Server Maintenance and Email Setup

This section describes how to perform Vocera Voice Server maintenance and configure email integration.

- **Performing Server Maintenance** on page 160
- **Email Setup** on page 175

Performing Server Maintenance

This section describes how to perform server maintenance, import and export data, update Vocera data, and check the Vocera database for potential problems.

Server Maintenance

Learn the tasks that can be performed on the Server page of Administration Console.

The Server page of the Administration Console lets you perform the following tasks:

- Manually backup data at any time. See Backing up and Restoring Data on page 160.
- Restore data that you have manually backed up or data that the system has backed up automatically. See Backing up and Restoring Data on page 160.
- Manually stop and start the Vocera Voice Server. See Stopping and Starting the Vocera Voice Server on page 161.

> **Important:** If you want to perform a system-level backup of Vocera Voice Server data outside of the Administration Console, make sure you follow the guidelines in Performing System-level Backups on page 162.

Backing up and Restoring Data

The Server page of the Administration Console lets you manually backup data or restore data that you have already backed up.

See Scheduling an Automatic Backup on page 112 for information about scheduling an automatic backup.

You should back up your data regularly to ensure its safety. Vocera lets you back up your data manually at any time, or automatically, at a time and interval that you specify. The backup operation does not stop the server or interfere with its use; you can perform the operation at any time.

If you need to restore data, you can choose from any backup file you have previously created. The restore operation briefly stops the server, empties all your existing data, then completely restores data from the backup file. The restore operation automatically logs out all your badges; users must log in again after the restore completes.

> **Note:** The backup and restore operations preserve all system data, including a cluster configuration, if one is specified. They also preserve application data for Staff Assignment.

Vocera backs up your data to a file in the **\vocera\backup** directory. The file is named with the following syntax, where **<MonDD>** is the three letter abbreviation of the month followed by the day, and **<HHMM>** is the time in 24-hour format:

backup-<MonDD>-<HHMM>.zip

For example, the following backup file was created on July 23rd, in the current year, at 1:45 PM:

backup-jul23-1345.zip

Backing up system data and restoring it may solve many data corruption problems. If you notice problems with your data and think that the database is corrupt, try backing up your data and immediately restoring it.

To back up data manually:

1. Click Maintenance in the navigation bar.
2. Click the Server tab to display the Server page.
3. Click the Backup button.

   Vocera backs up your configuration data to a file in the \vocera\backup directory and displays a dialog box showing you the progress. When the backup is finished, Vocera displays the progress as 100%.

4. Click OK to close the dialog box and return to the Administration Console.

To restore data from a backup that you have previously created:

1. Click Maintenance in the navigation bar.
2. Click the Server tab to display the Server page.
3. Click the Restore button.

   The Select File dialog box appears, displaying the list of available backup files in sequential order, with the most recent file at the top.

4. Select the name of the backup file that you want to use and click Restore.

   A warning appears, reminding you that the server stops and existing data is replaced when you restore data.

5. Click OK to close the warning and begin restoring data.

   Vocera displays a dialog box showing you the progress. When the operation is finished, Vocera displays the progress as 100%.

6. Click OK to close the dialog box and return to the Administration Console.

Stopping and Starting the Vocera Voice Server

In certain situations, you may need to stop and restart the Vocera Voice Server.

For example, if you want to use the server to update the properties in all your badges at the same time, you must stop the Vocera Voice Server and then restart it before it can download the new properties to the badges.

Use the Server page in the Maintenance screen to stop and start the Vocera Voice Server. The buttons in the Start and Stop Server section of the Server page control the Vocera Voice Server only; they do not stop the related services that Vocera uses, such as Tomcat and Nuance.

You may want to restart the server when only a few people are using the system. When you stop the server, any existing calls will be terminated, and users will not be able to communicate with their badges until you start the server again. The server stops and starts fairly quickly, so if few people are using the system, there will be very little interruption.

Note: You can also use the Vocera Control Panel to stop and start the Vocera Voice Server.

To stop and start the Vocera Voice Server

1. Open the Vocera Administration Console.
2. Click Maintenance in the navigation bar to display the set of Maintenance tabs.
3. Click the Server tab.
   The Server page opens.
4. Click the Stop.
   Vocera displays a dialog box indicating that the server has stopped.

5. Click OK to close the dialog box.

   The Server page is displayed again.

6. Click the Start button.

   Vocera displays a dialog box indicating that the server has started.

7. Click OK to close the dialog box.

Performing System-level Backups

All Vocera data (including messages and learned commands) is stored in the `\vocera\backup` folder, so you do not need to back up any other Vocera folders.

To back up Vocera Voice Server data, make a backup copy of the `\vocera\backup` folder.

> **Important:** **DO NOT** make a backup copy of the `\vocera\data` folder. Making a backup copy of the `\vocera\data` folder on the active node of a Vocera Voice Server cluster could cause the server to failover.

You should also make backup copies of the following properties files on the Vocera Voice Server and the Vocera SIP Telephony Gateway:

* `\vocera\server\properties.txt`
* `\vocera\config\badge.properties`
* `\vocera\telephony\vgw\vgwproperties.txt`

If you are planning to back up Vocera Voice Server data, make sure you do it AFTER the following Vocera Voice Server scheduled processes:

* The daily scheduled backup of Vocera data

   To schedule backup in the Administration Console, click System in the navigation bar, and then click the Backup tab.

* The daily scheduled sweep of Vocera messages

   To schedule sweep in the Administration Console, click System in the navigation bar, and then click the Sweep tab.

Importing Data from a CSV File

A CSV file lets you specify most of the information you can enter when you create an entry in the Administration Console.

When you enter data through the Administration Console, you use one of the Add dialog boxes to specify all the related information for a single entry. For example, to create a new user, you use the fields and tabs in the Add New User dialog box to provide user information, speech recognition, group membership data, and so forth.

If you need to enter a large amount of the same kind of data at a single time, however, it is faster to import it from a specially formatted CSV (comma separated value) file. For example, when you first load the Vocera database, it is often faster to import data for all your users from a single CSV file, rather than to create each user individually in the Administration Console.

> **Note:** The Vocera Voice Server supports CSV files up to 1 MB in size. If a CSV file that you want to import is larger than 1 MB, break it up into multiple files.

A CSV file lets you specify most of the information you can enter when you create an entry in the Administration Console. Each line in a CSV file represents a separate database entry. Within each line, commas separate the values that qualify the entry.

For example, each line in the CSV file you use to import user data represents a single user. Within each line, commas separate the values that you would enter in the fields and tabs of the Add New User dialog box.

About the Templates

The installation program provides templates that you use to create CSV files in the `\vocera\samples` directory of the Vocera Voice Server computer.

The templates are in Microsoft Excel format. Use these templates to enter the data you want to load, then save them in CSV format.

The following table lists the templates in the `\vocera\samples` directory:

Table 59: Import templates

Type of Data	Template
Sites	sites-template.xls
Groups	groups-template.xls
Users	users-template.xls
Group Members	groupmembers-template.xls
Address Book Entries	addresses-template.xls
Locations	locations-template.xls
Access Points	accesspoints-template.xls
Devices	devices-template.xls

If you are loading all your data from spreadsheets, you must use the spreadsheets in the order shown in the above table. The data in the later spreadsheets has dependencies on the data you load earlier, and it may fail to load if you do not follow this sequence.

When you import Vocera groups, DO NOT import the Forwarding field in the first pass.

Note: Vocera supports numeric values that begin with zero such as 01234 in name fields. However, Excel strips initial zeros from numeric values without warning. If you want to use numeric values that begin with zero in name fields, do not use Excel to edit your `.csv` files. Instead, use a different spreadsheet program, such as OpenOffice Calc (http://www.openoffice.org/).

Sites and Templates

Learn about using templates for site data.

You reference site data in the templates in two different ways:

- To assign an entity you are creating to a site, use the *Site* column in the template.

  For example, to create a user called Lin Yao and assign her to the San Francisco site, enter `San Francisco` in the *Site* column of `users-template.xls`.

- To qualify a value in a specific spreadsheet column by specifying its site, use a colon to separate the value from the site name (Value:Site name).

  For example, to specify that the Tech Support group is at the Santa Cruz site, enter `Tech Support:Santa Cruz` in the *Group Name* column of `groupmembers-template.xls`.

The following table lists template fields that support the Value:Site syntax:

Table 60: Template fields that support Value: Site syntax

Template	Field (s)	Default Site
groups-template.xls	Forwarding Manager Group Add Group Device Group	the value in the *Site* field
users-template.xls	Conference Group	the value in the *Site* field
groupmembers-template.xls	Group Name	Global

Template	Field (s)	Default Site
`accesspoints-template.xls`	Location Name	Global
`devices-template.xls`	Owning Group	Global

Preparing CSV Files

Learn the steps to follow in order to prepare a spreadsheet file.

Each column in a template corresponds to a field in the associated Add/Edit dialog box. Create new rows in the template by supplying appropriate values in the fields under each column. After you finish entering data, replace all empty cells in the spreadsheet with a space to ensure that the cells will be included in the CSV. When you are finished, delete the header row, and save the template as a CSV file.

To prepare a CSV file:

1. Open the appropriate template in Microsoft Excel.
2. Provide information for each entry you want to import on a separate row of the spreadsheet. For example, if you are importing user data, you provide information for each user on a separate row of the `users-template.xls` spreadsheet.

   See the *Vocera Voice Server Data-Loading Reference* for information about the data you should provide.
3. When you finish entering data, follow these steps to replace all empty cells in the spreadsheet with a space.

   Note: If the last column of data in your spreadsheet is empty, Excel produces inconsistent results when you save to CSV. These steps provide a simple workaround and ensure that all empty cells will be included in the CSV.

   a. Select a cell in the header row.
   b. Press Ctrl+A to select the current region.
   c. Choose Edit > Replace. The Find And Replace dialog box displays, with the Replace tab selected.
   d. Make sure the Find What box is completely empty.
   e. In the Replace With box, enter a single space.
   f. Click Replace All.
      A message box displays showing how many replacements were made. Click OK.
   g. Click Close to close the Find And Replace dialog box.
4. Delete the row of column headings—you do not want to load the headings into the Vocera database.
5. Save the spreadsheet as a CSV file:
   a. Choose File > Save As. The Save As dialog box displays.
   b. In the Save As Type drop-down list, select CSV (Comma delimited).
   c. In the File Name box, type the filename.
   d. Click Save.

Importing Text into Microsoft Excel

If you use Microsoft Excel to edit data that you exported from Vocera, the program may automatically change some values into Number or Date format.

To prevent Excel from changing the format of values, import the data into Excel as text.

Note: To avoid data conversion problems caused by Microsoft Excel, use a different spreadsheet program, such as OpenOffice Calc (http:// www.openoffice.org/).

To import text into Microsoft Excel:

1. Change the filename extension of the file you exported from Vocera from `.csv` to `.txt`.

2. Start Microsoft Excel.

3. Open the file that you renamed in step 1.
   The Text Import Wizard appears.

4. In the Original Data Type box, select Delimited. Click Next.
   Step 2 of the Text Import Wizard appears.

5. In the Delimiters box, make sure only Comma is checked. Click Next.
   Step 3 of the Text Import Wizard appears.

6. In the Data Preview box, select all columns. To do this, follow these steps:
   a. Click the column heading for the first column.
   b. Use the horizontal scrollbar to scroll to the last column.
   c. Press and hold the Shift key, and then click the column heading for the last column.
   All columns should now be highlighted in black.

7. In the Column Data Format box, select Text. Click Finish.
   The data is imported as text.

Importing Groups in Multiple Passes

Learn basic information about importing multiple groups.

Because the Forwarding field in the groups template (`groups-template.xls`) allows you to reference other Vocera entities, such as users, Address Book entries, and other groups, it is important to validate group data before you try importing it. If a group record references a user or Address Book entry that does not exist in the Vocera database, the record will be skipped when you try to import it.

> **Note:** When you reference other groups within a group record, the referenced group does not need to exist in the database as long as it is defined as another record in the same import file.

To avoid data validation errors, Vocera recommends importing group data in multiple passes. On the first pass, DO NOT include the Forwarding field in your import data. Once groups are successfully imported, continue importing other Vocera entities, such as users and Address Book entries. After users and Address Book entries have been imported, you can use the Update page of the Administration Console to update groups with the Forwarding data. See Updating Users, Groups, and Devices with CSV Files on page 167.

Validating and Importing Data

Learn about importing data from a CVS file.

After you have finished preparing the CSV files, use the Import page of the Maintenance section in the Administration Console to load the database. Vocera lets you validate the data in your CSV file before you import it:

- When you validate data, Vocera examines each row in the CSV file to confirm that it is formatted correctly. Vocera reports any errors, provides details to help you correct the errors, and lets you fix the problems before importing.

- When you import data, Vocera loads each row in the CSV file that is formatted correctly. Vocera flags any rows that have errors, reports the type of error, and does not load the data in the problem rows.

Even if you import data without validating it, Vocera will not let you corrupt the database with incorrectly formatted data. However, it is usually more convenient to validate the data before importing it.

To import data from a CSV file:

1. Click Maintenance in the navigation bar.

2. Click the Import tab to display the Import page.

3. Specify the type of data to load in the Import Data from a File section.

4. Click Browse and navigate to choose a CSV file to import data from.

5. Do either of the following:

   • Click Validate to examine the data for errors without importing it.

   • Click Import to load the data immediately.

   Vocera displays a dialog box showing you the progress of your action. When the validation or update is finished, Vocera displays the progress as 100 percent.

6. If necessary, click Show Errors to display the Errors dialog box. Vocera provides details to help you correct the error. When you are finished reviewing errors, click OK to close the Errors dialog box.

7. Click OK to close the Progress dialog box.

Exporting Data to a CSV File

You may occasionally want to export large sets of data from the Vocera database to a CSV file.

Exporting data is useful when you want to examine all your data or make global changes that would be time consuming to make in the Administration Console.

For example, suppose changes to the phone system caused your organization to reassign desk extensions for all users. You can export the existing user data to a CSV file, make the changes to desk extensions, and then use the Update feature to replace the existing user data with the data in your CSV file.

Exporting data does not remove it from the database. See **Emptying the Vocera Database** on page 169.

> **Note:** Vocera supports numeric values in name fields. The Administration Console lets you create a purely numeric name that begins with a zero, such as `01234`, and exports it to a .csv file correctly. However, Excel strips initial zeros from numeric values without warning. If you are using numeric values that begin with zero in name fields, do not use Excel to edit your .csv files.

To export Vocera data:

1. Click Maintenance in the navigation bar.

2. Click the Export tab to display the Export page.

3. Use the Site filter to specify which site to export data from.

4. Specify the data to export in the Export Data to File section.

5. Click Export.
   Windows displays the File Download dialog box.

6. Specify whether to save the file or to open it for viewing:

   • Click Open to view the file. You can open a CSV file in Microsoft Excel, a text editor, and many other applications.

   • Click Save to browse to a location and enter a file name for the file.
     The data you export is in CSV format, appropriate for importing again.

   > **Note:** Only users, groups, and devices can be updated by importing a CSV file. Other types of Vocera entities can be imported only once.

Updating the Vocera Database

This section describes how to update Vocera data from a CSV file.

Updating Users, Groups, and Devices with CSV Files

When you update Vocera data with data from a CSV file, you must specify key fields to indicate which Vocera database record to update.

The following table lists key fields for users, groups, and devices:

Table 61: Key fields for updating records

Data Type	Key Field(s)
User	User ID
Group	Group Name Site
Device	MAC Address

You cannot use CSV files to modify key fields—you must edit those fields manually in the Administration Console.

When you use CSV files to update the database, the CSV data must be formatted as described in About the Templates on page 163.

You typically export existing user, group, or device data to a CSV file, edit the CSV file, and then use the update feature to copy data from the CSV file back to the Vocera database. For each row in the CSV file, new field values overwrite corresponding values in the database, blank field values leave the corresponding database values unchanged, and the literal string value ***blank*** in a CSV row erases the corresponding value in the database.

For example, suppose a user profile in the database includes the following data:

User ID	Last Name	First Name	Identifying Phrase	Email Address
jsmith	Smith	John		jsmith@xyz.com

Next, suppose a row in a CSV file contains the following field values:

```
jsmith, , Jack, , *blank*
```

When you upload the CSV file, the value of the User ID field specifies which database record to update, the values of the Last Name and Identifying Phrase fields are not changed, the value of the First Name field is changed from John to Jack, and the value of the Email Address field is erased (empty).

To update user, group, or device data with CSV files:

1. Prepare a CSV file for the data you want to update or delete.
2. Click Maintenance in the navigation bar.
3. Click the Update tab to display the Update page.
4. In the Update box, click either Users, Groups, or Devices to specify the operation you want to perform.
5. Click Browse and navigate to select the CSV file you want to use.
6. Do either of the following:
   - Click Validate to examine the data in the CSV file for errors without modifying the database.
   - Click Update/Delete to update records in the database immediately.
     Vocera displays a dialog box showing you the progress of your action. When the action is finished, Vocera displays the progress as 100%.
7. If necessary, click Show Errors to display the Errors dialog box. Vocera provides details to help you correct the error. Review any errors, then click OK to close the Errors dialog box.
8. Click OK to close the Progress dialog box.

Deleting Users or Devices with CSV Files

Learn the steps for deleting users or devices from the CVS file.

When you use CSV files to delete users or devices from the database, the only required value in each row of the CSV file is the first value. For users, the first value is the user ID. For devices, the first value is the MAC address.

If other data exists in the row, the first value must be followed by a comma. When you use the delete feature, all data related to the user or device is deleted from the database, not just the data that is specified in the CSV file.

To delete users or devices with CSV files:

1. Prepare a CSV file for the data you want to delete.
2. Click Maintenance in the navigation bar.
3. Click the Update tab to display the Update page.
4. In the Delete box, click either Users or Devices to specify the operation you want to perform.
5. Click Browse and navigate to select the CSV file you want to use.
6. Do either of the following:
   - Click Validate to examine the data in the CSV file for errors without modifying the database.
   - Click Update/Delete to delete records in the database immediately.

     Vocera displays a dialog box showing you the progress of your action. When the action is finished, Vocera displays the progress as 100%.
7. If necessary, click Show Errors to display the Errors dialog box. Vocera provides details to help you correct the error.
8. Review any errors, then click OK to close the Errors dialog box.
9. Click OK to close the Progress dialog box.

Merging Device Data with CSV Files

With the Merge feature on the Update page, you can add new devices and update existing devices from a CSV file in one operation.

This is important because Vocera automatically loads any new devices when they connect to the server. Therefore, you can use the autoload feature to get all of your active devices entered into the system, export the device information as described in **Exporting Data to a CSV File** on page 166, combine the data with data from your previous badge inventory system, and then merge the data back into Vocera. Any new devices are added and existing devices are updated.

For each row in the CSV file, if the MAC address is new, a new device is added to the Vocera database. If the MAC address already exists in the Vocera database, new field values overwrite corresponding values in the database, blank field values leave the corresponding database values unchanged, and the literal string value ***blank*** in a CSV row erases the corresponding value in the database.

> **Important:** You must specify a value in the MAC Address field (the first field in the CSV file) to indicate which Vocera database record to update. Otherwise, the record is skipped.

To merge device data with CSV files:

1. Prepare a CSV file for the data you want to add and update.
2. Click Maintenance in the navigation bar.
3. Click the Update tab to display the Update page.
4. In the Merge box, click Devices to specify the operation you want to perform.
5. Click Browse and navigate to select the CSV file you want to use.
6. Do either of the following:

- Click Validate to examine the data in the CSV file for errors without modifying the database.
- Click Update/Delete to update records in the database immediately.

Vocera displays a dialog box showing you the progress of your action. When the action is finished, Vocera displays the progress as 100%.

7. If necessary, click Show Errors to display the Errors dialog box. Vocera provides details to help you correct the error.

    Review any errors, then click OK to close the Errors dialog box.

8. Click OK to close the Progress dialog box.

Emptying the Vocera Database

You can use the Update page to empty all of the custom data you have entered into the Vocera database, returning it to its default condition.

If you perform this procedure, you will need to restore your data from a backup file or set Vocera up again before users can communicate with their badges.

When you empty the Vocera database, you remove any settings you have made and delete any data you have entered. The database is restored to the condition it was in immediately after your installation. The Vocera Voice Server automatically stops and then restarts when you empty the database.

> **Important:** Back up your database before emptying your data from it. You cannot restore data after you have emptied it unless you first create a backup file. See **Backing up and Restoring Data** on page 160.

The Vocera Voice Server automatically stops and then restarts when you empty the database.

To empty the Vocera database:

1. Click Maintenance in the navigation bar.
2. Click the Update tab to display the Update page.
3. Click the Empty button.

    A dialog box warns that you cannot undo this procedure.
4. Click OK.

    The warning dialog box closes, and Vocera displays status messages while it empties the database.
5. When the database is emptied, you are prompted that the operation completed. Click OK to close the dialog box.

Checking Data

The Data Check page of the Administration Console lets you check your database for potential problems that could impact usability of the system.

The Data Check only runs when an administrator invokes it.

When running the Data Check, start by running one option at a time to make the resulting report easier to work with.

The Data Check flags items found during its search with either a High, Medium, or Low severity flag. High Severity items are ambiguous choices that cannot be resolved by a badge user during a call, while Medium or Low severity items can be resolved. A few examples of various types of flagged items are shown below.

To check your data manually:

1. Click Maintenance in the navigation bar.
2. Click the Data Check tab to display the Data Check page.

3. Select one or more checkboxes for the data types to check:
   - Names
   - Phone Numbers
   - Groups
   - Departments

   Note: You should only check one checkbox at a time to make the report manageable. If you run the Data Check for names and the report seems unusually large, go to the Systems screen and temporarily uncheck the "First Name and Department" checkbox in the Preferences tab. Be sure to click Save Changes before returning to the Data Check to run the report again.

4. Click the Check button.

   Vocera checks your data and displays the results in the Data Check Warnings dialog box. See Data Check Warnings on page 172 for additional information.

Checking Names

When checking names, the Data Check is looking for situations which result in ambiguous choices when a user issues a voice command.

This can include either of the following situations:

- Two (or more) badge users with the same first name in the same department, when "First Name and Department" is enabled as a System Preference.

  For example, if Seymour Krelborn and Seymour Puddle work in the Produce department, *and* the "First Name and Department" setting is enabled in System Preferences, a voice command to "Call Seymour in Produce" would result in two possible targets for the call.

  This is an ambiguous choice, as further clarification from the caller is required when calling "Seymour in Produce" (the user can respond to the full name of each possible choice when the Genie asks for clarification).

  The Data Check would flag this item with Low Severity, as having a spoken name in common. Fixing Low Severity items can wait until you have time to investigate and resolve them, as they do not prevent communication from occurring. However, they do result in annoying "Do you mean so-and-so?" questions for system users, which may lower their satisfaction and reduce the overall usage level of the system.

  Similarly, any two non-user entities with the same Spoken Name will be flagged with Low Severity. For example, if two groups, "Info Services" and "I T" share the spoken name "I T", they will be flagged with Low Severity (again, when the Genie asks for clarification the user can distinguish between the possibilities using the full name of each group).

- Two (or more) names (users, buddies, and address book entries) with the exact same spoken name (first and last names for people).

  When two users have the same first and last names (e.g. "Joe Fox"), they will be flagged with High Severity, as there is no way for a user calling Joe to tell them apart.

If you have enabled calling by first name and department on the Preferences page of the System screen, the Data Check report may display a large number of conflicts. For example, the users Seymour Glass and Seymour Franklin may have the spoken name "Seymour in Produce" in common. Depending on the size of your departments, your report may display many speech recognition conflicts in this form.

If your data check report contains many first name and department conflicts, you can fix the problem in either of the following ways:

- Temporarily uncheck "First Name & Department" in the System Preferences tab and run the report to filter these speech recognition errors. Turn the feature on again immediately, because turning it off for more than a few moments on a production system may confuse users.

After fixing other speech recognition conflicts, run the report again and fix the "First Name & Department" conflicts.

- Permanently disable the call by first name and department feature.

  If this feature results in too many errors, disable it and require users to call by first name, last name, and department.

Buddy Names and the Data Check

One user's buddy name will not conflict with another user's buddy name (even for the same person), but there will be a conflict with any Alternative Spoken Name that is the same.

For example, Jane has recorded a buddy name of Dad for her father Steve, and Christopher, another badge user, has an Alternative Spoken Name of Dad. Jane calls Christopher on business and later calls her Dad to meet for dinner. She will be asked if she means Steve, because there are now two entries for Dad: her own Buddy, and Christopher's Alternative Spoken Name.

Correcting Name Items

Items with a High Severity should be investigated immediately, and resolved in conjunction with the users involved.

Possible resolutions include:

- If multiple user profiles exist for one person, consult with the person to determine which one is used regularly, and remove the others.
- Where two different people have the exact same name, consult with them to create unique identifying phrases for each of them.
- Where two different people share the same Alternative Spoken Name, consult with them to create unique Alternative Spoken Names for each of them.

Checking and Correcting Phone Numbers

When checking phone numbers (extensions), the Data Check is looking for situations where more than one entry in the database has been assigned the same phone extension.

This includes users, groups, or address book entries being assigned an extension that has been previously assigned to any other entity. All phone items found are flagged with High Severity. The Data Check checks the "Desk Phone or Extension" and "Vocera Extension" fields for users, and the "Vocera Extension" field for groups. Matching phones between different address book entries are not flagged.

You must change one of the duplicate phone numbers, or the first entity assigned an extension number will receive all calls for any entity assigned that number.

For example, the groups "Engineers" and "Facilities" (who share the same physical office) have both been assigned extension 6543, as has Tom Swift, the head engineer. If someone attempts to call Tom using extension 6543, the call may be routed to the Engineering group instead of his desk phone.

Desk extensions must be unique. If the users have actual desk phones, these numbers are already unique. If you are in an environment that does not have desk phones, extensions are used for paging callbacks, and still must be unique. For complete details, see the Desk Phone and Extensions discussion at **About Users and Telephone Numbers** on page 50.

There is one situation in which changing one of the matching extensions is not needed—when two different group names represent the same group; in other words, one group is a duplicate. In that case, you should remove the duplicate group (after consulting with its members) and consider creating the duplicate name as an Alternative Spoken Name of the surviving group.

Checking and Correcting Group Items

Learn about Data Check for group checks.

When checking groups, the Data Check is looking for any of the following situations:

- Department groups nested within other department groups
- Groups with no members that have not been set to automatically remove members (Temporary Membership groups)
- Groups without a forwarding phone number
- Users who belong to no groups other than Everyone

Nested department groups will receive a High Severity flag; the other situations will be flagged as Low Severity.

Do not nest departments—it can confuse users and generate unintended results in the Report Server. Please read the section on Departments at **About Groups and Departments** on page 70.

As discussed in **About Speech Recognition** on page 204, every group adds between three and six spoken names to the system. Groups that have no members can add significantly to the overall spoken name count, while contributing nothing to the system. If you have an empty group, be sure that you want it to exist, otherwise remove it.

Groups with no forwarding setting will prompt a caller to leave a message; that message is delivered to all members of the group. This could lead to multiple callbacks, or worse, no callbacks if every group member assumes someone else returned the call. To resolve these items, set forwarding for the group to a badge, address book entry, or another group.

Users who are not members of any groups (other than Everyone) may represent duplicate user entries, new users who were not completely set up in the system, or former users who have not been completely removed from the system. Contact the users' managers to see if they still need access to Vocera, and what groups they should be made members of.

Checking and Correcting Departments

Learn about Data Check checking for departments.

When checking departments, the Data Check is looking for any of the following situations:

- Departments that have been nested within other departments
- Departments that are unusually large or small (more than 1000 members or fewer than 3 members)
- Departments that have no members
- Users that have not been assigned to any departments

Nested department groups will receive a High Severity flag; the other situations will be flagged as Medium or Low Severity.

Data Check Warnings

Learn about Data Check warnings.

The Data Check Warnings dialog box displays a report for the names, phone numbers, and groups in your database that may result in speech recognition problems. The Data Check Warnings dialog box appears when you select an item on the Data Check page of the Maintenance screen and click Check. The maximum number of warnings that can be shown is 3,000 but total number of warnings that Vocera reports is 300,000.

When the Data Check Results window is open, you cannot switch between the report and the console to make changes. Therefore, you should click the Printable Format button to open the printable version of the report in a new window, then click Close in the modal window to return to the Console window.

In addition, you can export the warnings to a spreadsheet by clicking Export. Using the export function is preferred if the configuration errors exceeds 3,000 warnings since the Data Check window and the printable format option limit the number of viewable return results. The number of warnings is listed at the bottom of the Data Check Results window which can assist you in determining if you should use the export function or simply view a limited number of errors in Administration Console UI.

Switch to the Printable Report window and either print the report for your reference or horizontally tile the Console and Report windows on your desktop so you can work in the Console while viewing the report.

> **Note:** The Data Check window and the Printable Report window contain the same data but are limited to 3000 return results. Use Export to view all the results for a larger number of warnings.

Table 62: Data Check fields

Field	Description
Warning	This column lists the entities found with settings flagged by the Data Check.
Action Required to Resolve Issue	This column displays the recommended step to resolve the problem found by the Data Check.
Severity	This column displays the Severity level for the problem, either a High or Low severity flag. High Severity items are ambiguous choices which cannot be resolved by a badge user during a call, while Low severity items can be resolved.

Working with Server Log Files

Log files provide important data and other system measurments.

The Vocera Voice Server maintains four sets of log files in the `\vocera\logs` directory:

- System logs record general system events for trouble shooting.
  The names of these files begin with the **log** prefix.
- Report logs record data that the Vocera Report Server uses to create reports.
  The names of these files begin with the **report** prefix.
- Tomcat logs record events related to the Tomcat server used by Vocera.
  These files are in the `\vocera\logs\tomcat` subdirectory.
- Nuance logs record events related to the Nuance speech engine used by Vocera.
  These files are in the `\vocera\logs\Nuance` subdirectory.

Both Vocera SIP Telephony Gateway and Vocera Client Gateway maintain log files in their own `\vocera\logs` directory. The names of these files begin with the **vtg** and **vcg** prefixes, respectively. The names of debug-level logs, which have more detail than the console logs, begin with the **vtg-dlog** and **vcg-dlog** prefixes, respectively.

Vocera Voice Server log files have the following syntax, where **<log>** indicates the type of log file, **<YYYY>** is the four-digit year, **<MM>** is the two letter abbreviation of the month, **<DD>** is the day, and **<HHMMSS>** is the time in 24-hour format:

<log>-<YYYY>-<MM>-<DD>-<HHMMSS>.txt

For example, the following log file was created on 4-July-2014 at 11:30 PM and 28 seconds to record system events:

log-2004-07-14-233028.txt

When the Vocera Voice Server starts, it creates one log file to record system events and a separate log file to keep track of data for the Report Server. By default, the server continues to write data to a log until the file reaches 100,000 lines or until the server stops. At that time, the server closes the file and opens another one. The server also closes each log file and starts another one at midnight.

By default, the Vocera Voice Server saves up to 100 system logs and 100 report logs. If the number of either type of log will exceed 100, the server deletes the oldest file and saves the most recent one, so there are never more than 100 of any type of log.

Similarly, the Vocera SIP Telephony Gateway and Vocera Client Gateway maintain up to 100 logs of up to 100,000 lines each.

Email Setup

Email configuration extends the reach of the Vocera Communications system into the Internet, allowing the Vocera Voice Server to send alert messages to any email address, and enabling badge users to send voice email messages to any user, group, buddy, or address book entry with an email account.

Vocera email settings are divided into three categories:

- Host Info settings identify your mail server so your Vocera Voice Server can communicate with it successfully.
- Mailbox settings let you identify the mailboxes and hosts for incoming and outgoing mail.
- Alerts settings let you specify recipients for outgoing log and alert mail messages from the Vocera Voice Server.

Email settings are site-independent: they affect email for all your sites. You configure email settings in the Email screen of the Administration Console.

Sending Email Alert Messages

An alert message is an email that the Vocera Voice Server can optionally send to notify you about events in your system.

These include:

- The amount of free disk space on the Vocera Voice Server drive is less than or equal to 3000 megabytes (the default threshold set as the value of **SysFreeDiskSpaceWarningThreshold** in `\vocera\server\properties.txt`.)
- The Vocera Voice Server stopped because the amount of free disk space is less than or equal to 1500 megabytes (the default threshold set as the value of **SysFreeDiskSpaceStopThreshold** in `\vocera\server\properties.txt`.)
- The memory in use is within 100 megabytes of the maximum amount of heap memory Java can allocate from the operating system.
- The Vocera Voice Server restarted because the amount of memory in use is within 50 megabytes of the maximum amount of heap memory Java can allocate from the operating system.

  > **Note:** This is a fast restart that releases memory and allows the system to continue running without causing a failover.

- The active node of a Vocera cluster failed, resulting in a failover.
- One of the standby nodes of a Vocera cluster failed.
- The number of logins exceeds 90% of the login license limit (if there is one). One email alert is sent each day the login license threshold is exceeded. The 90% (.90) threshold is the default value of **SysLoginLicenseAlertThreshold** in `\vocera\server\properties.txt`.
- The Vocera license is within 5 days of its expiration date. You receive an additional warning each day until the license is renewed or expires.

- The Vocera Voice Server stopped running because its license expired.
- The Vocera Voice Server is unable to connect to the Vocera SIP Telephony Gateway, or Vocera Client Gateway, whether it is a single server or a member of an array.
- The Vocera Voice Server reconnected to a Vocera SIP Telephony Gateway.
- The Vocera Voice Server was unable to establish a connection to the Active Directory. By default, another email alert is sent every 30 minutes until the connection is successful.
- The Vocera Voice Server connection to the Active Directory went down.
- The Vocera Voice Server connection to the Active Directory has switched from a primary server to a secondary server. You may need to take corrective action to ensure that a primary Active Directory server is running and is accessible over the network. By default, another email alert is sent every day until the connection to a primary server is successful.
- The Staff Assignment application changed a department or subdepartment group to an ordinary group. This alert is for information purposes only. Corrective action may not be necessary.

Each email alert includes general information about the Vocera Voice Server, including the IP address of the host, Vocera cluster members, when the alert was generated, to whom the

Sending Voice Email

Badge users can send a voice email by commanding the Genie to "Send email to person's first and last names," and then recording a message.

A voice email is an email message with a .WAV file attached that contains the voice message. The Vocera Voice Server checks the recipient's profile and sends the voice email as an attachment to a text email.

The following illustration shows the process of sending a voice email message from a badge:
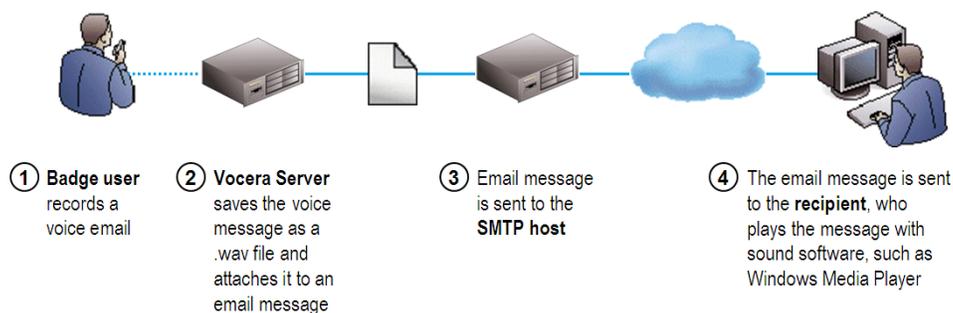
Figure 17: Sending a voice email message from a badge

In the above illustration:

1. A badge user records a voice message.
2. The Vocera Voice Server saves the recording as a .WAV file and attaches it to an email message.
3. The email message is sent to the SMTP host.
4. The email message is sent to the recipient, who plays the message with sound software such as Windows Media Player.

See the *Vocera User Guide* for information about sending email messages from badges.

Sending Email Messages to Vocera Devices

The figure in this topic outlines the process for sending short, plain text or HTML email messages to Vocera devices.
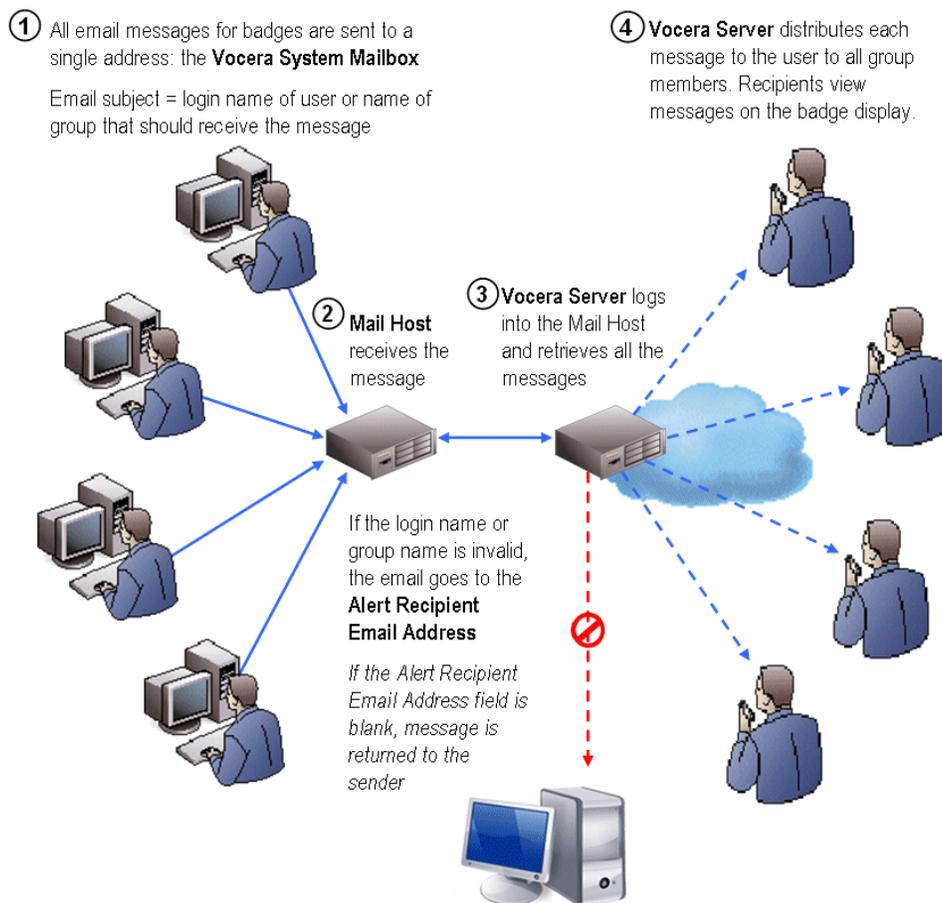
Figure 18: Sending email messages to Vocera devices

In the above illustration:

1. All email messages for Vocera devices are sent to a single address, the Vocera Mailbox. Email subject is a user ID or the name of the group that should receive the message. If the user ID or group name is invalid, the email goes to the Alert Recipient Email Address. If the Alert Recipient Email Address is not defined, the message is returned to the sender.

2. Mail host receives the message.

3. Vocera Voice Server logs in to the Mail Host and retrieves all the messages.

4. The Vocera Voice Server distributes all the messages, and recipients view them on their Vocera devices.

To send a text message to Vocera devices from an email account:

1. In your email program, start a new message.

2. In the **To:** field, enter the email address of the Vocera system.

3. In the Subject: field, specify the message recipient using one of the following formats:

    - The user ID of a Vocera user. For example:

      `jbatista`

    - The name of a group, if the group is in the global site. For example

      `I C U Nurses`

    - The name of a group and its site, if the group is in any other site. Specify the group name in brackets, followed by the site name in braces. For example:

      `[I C U Nurses] {West Wing}`

- With Vocera 4.3 (or later), you can send an urgent text message via email. To send an urgent message, include the string **urgent** anywhere in the subject, and specify the ID of a Vocera user or a group name in brackets. If the user or group is not in the Global site, also specify the site in braces. For example:

```
[jbatista] **urgent**
[I C U Nurses] {West Wing} **urgent**
```

4. In the **message area**, type your message. Be brief, because the message will be limited to 223 characters on Vocera badges or smartphones, and 236 characters on a Cisco Unified Wireless IP Phone (7900 series). Additional characters will not be displayed.

> **Note:** When the recipient views the list of text messages, the entry for an email will show the first thirteen characters of the message.

5. Make sure the email message is formatted as plain text or HTML. RTF formats are **not** supported.

6. Send the email message in the usual way.

The Vocera Voice Server logs in to the Vocera system email account at regular intervals (usually every 30 seconds), downloads all the email in the mailbox, and distributes each message to the user or group whose user ID or group name appears on the subject line of the message.

See the Vocera B-Series Badge User Guide for information about reading email messages on the badge display.

Configuring Email Settings

Email settings are site-independent: they affect email for all your sites.

Use the Email screen to specify the following settings:

- Your mail server
- Mailboxes used for incoming and outgoing mail
- Recipients for Vocera Voice Server alerts

Configuring Host Info Settings

Host Info settings identify your mail server so the Vocera Voice Server can communicate with it successfully.

Table 63: Mail host information settings

Field	Maximum Length	Description
Mail Host	60	In the Mail Host field, enter the name of the POP or IMAP server that receives and stores your email. Example: **mail.yourcompany.com**. The host that you specify in this field is used for incoming mail. By default, the Vocera Voice Server also uses it for outgoing mail unless you specify otherwise in the SMTP Host field. See Outgoing Mail Settings on page 180. **Note:** If you select EWS as your mail server type, an Exchange Web Service URL must be configured and added it to the Mail Host field. For example, `https://outlook.office365.com/EWS/Exchange.asmx`. Be aware that the EWS URL values for your organization may differ from the provided example.

Field	Maximum Length	Description
Mail Host Domain Name	60	In the Mail Host Domain Name field, specify the domain name used in email addresses at your site. Entering a value for this field ensures that anyone can reply to email sent from the badge. Example: **yourcompany.com**.
Mail Server Type	n/a	Choose the Mail Server Type that matches the protocol supported by your email server. These include: • POP3 (Post Office Protocol 3) • IMAP (Internet Message Access Protocol) • EWS (Microsoft Exchange Web Service) If you select EWS as your mail server type, please be aware of the following: • For Staff Assignment customers: In the Vocera Server Admin Console, go to Email -> Mailbox and select the checkbox next to Enable SMTP Authentication. If this field is left blank and not selected, credentials are not provided to Staff Assignment which will not work as expected. • For Vocera Report Server customers: When EWS is selected for Vocera Voice Server, then you cannot load the mail server settings from the Vocera Voice Server to the Vocera Report Server. Go to Administration -> Mail Info and uncheckbox next to Download Mail Setup from Vocera Server . In this instance, your email should either be disabled or you must provide separate SMTP information.

To configure email host settings:

1. Click Email in the navigation bar.
2. Click the Host Info tab.
3. Enter information identifying your mail server.
4. Click Save Changes.

Configuring Mailbox Settings

The Mailbox page lets you identify the mailboxes to use for both incoming and outgoing mail.

Incoming Mail Settings

Incoming mail is conventional email that anyone can send to a badge user.

Email messages appear as text on the display screen of the badge. Users can either read the message or listen to it as Vocera converts it to speech. See the *Vocera Badge User Guide* for complete information about receiving email messages on the badge.

Incoming Mail Settings enable the Vocera Voice Server to log in to an email mailbox reserved for the Vocera system and retrieve email messages intended for badge users. The Vocera Voice Server software then routes each message to the badge display of the recipient whose user ID appears in the subject line of the message.

Table 64: Incoming mail settings

Field	Maximum Length	Description
Vocera Mailbox Login ID	50	In the Vocera Mailbox Login ID field, enter the address or ID of the Vocera mailbox that the IT administrator reserved for email sent to Vocera devices (vocerabadge@yourcompany.com, for example). The Login ID may either be a full e-mail address (such as vocerabadge@yourcompany.com), or just the login ID part of the address (vocerabadge, in this case). Check with the IT administrator to find out which of these conventions was used.

Field	Maximum Length	Description
Password	15	In the Password field, enter the password the Vocera Voice Server must use to log in to the Vocera mailbox. Type the password again in the Re-enter Password field to ensure that you typed it correctly.
Mail Check Interval	n/a	The Mail Check Interval field specifies the time in seconds that the system waits between mail checks. During a mail check, the Vocera Voice Server connects with the Mail Host to check for new mail. Enter a value between 15 and 90 seconds; the default is 30.

To configure incoming mail settings:

1. Click Email in the navigation bar.
2. Click the Mailbox tab.
3. Enter your incoming mail settings.
4. Click Save Changes.

Outgoing Mail Settings

Learn about the available setting for outgoing mail.

Outgoing mail includes:

- Alerts that the Vocera Voice Server automatically sends to notify you of significant system events.
- Voice messages that badge users can send as email attachments. The Vocera Voice Server saves the voice message as a .WAV file and attaches it to a text email message containing instructions on how the recipient can reply to the message.
- Conventional email messages, sent from outside the Vocera system and intended for badge users, but with invalid recipients. If an incoming email specifies an invalid Vocera user ID or group name, the Vocera Voice Server uses the outgoing mail settings to send the email to the address specified in the Alert Recipient Email Address field. If you do not specify this value, the Vocera Voice Server uses the outgoing mail settings to return the message to the sender.

> **Important:** You must specify recipients for outgoing email on the Alerts page of the Email screen. See **Configuring Alerts Settings** on page 181.

Table 65: Outgoing mail settings

Field	Maximum Length	Description
SMTP Host	60	Enter the name of the server used for outgoing mail in the SMTP Host field. For example: **mail.yourcompany.com**. If you do not enter a value in this field, Vocera uses the value of the Mail Host field. See **Configuring Host Info Settings** on page 178.
SMTP User Name	50	Enter the user name or address used to login to the outgoing mail server in the SMTP User Name field. Enter a value in this field only if it is different from the Vocera Mailbox Login ID value in the Incoming Mail Settings. The SMTP User Name will be different from the Vocera Mailbox Login ID only if your mail service provider requires different user names for sending and receiving mail.
Password	15	Enter the Password only if it is different from the value in the Password field in Incoming Mail Settings. If you enter a password, enter it again in the Re-enter Password field to ensure that you typed it correctly.
Enable SMTP Authentication	n/a	Check Enable SMTP Authentication if your mail server requires its subscribers to provide authentication when sending an email message.

Field	Maximum Length	Description
Test Outgoing Settings	n/a	Click Test Outgoing Settings to send a test message to the specified default alert recipient. After you click Test Outgoing Settings, a dialog box appears saying whether the email test was successful.

To configure outgoing mail settings:

1. Click Email in the navigation bar.
2. Click the Mailbox tab.
3. Enter information for your outgoing mail server.
4. Click Save Changes.

Configuring Alerts Settings

The Alerts page lets you specify recipients for outgoing mail sent by the Vocera Voice Server.

For example, you can specify an address that the Vocera Voice Server uses to send notifications of significant system events.

> **Important:** You must set up the outgoing email server on the Mailbox page of the Email screen, either by configuring it explicitly or by configuring incoming mail settings that it shares, before Vocera can send any email. See **Outgoing Mail Settings** on page 180.

Table 66: Alert settings

Field	Maximum Length	Description
Alert Recipient Email Address	50	In the Alert Recipient Email Address field, enter an email address to receive warning messages that the Vocera Voice Server can issue. The Vocera Voice Server sends alert messages to notify you of significant system events, such as low disk space and cluster failovers. For a list of possible alerts, see **Sending Email Alert Messages** on page 175. This address also serves as the destination for all email messages incorrectly addressed to badge users. These email failures are usually caused by an incorrect Vocera user ID on the subject line of the message. You can optionally re-route the email by correcting the subject line and resending the message. If this field is empty, you won't get any alerts, and email that fails to reach recipients is returned to the sender. > **Important:** Make sure the address you enter in this field: • Is different from the address used in the Vocera Mailbox Login ID field. • Does not forward to the address in the Vocera Mailbox Login ID field. Otherwise, non-deliverable email will loop between the two addresses until either the mail server or the Vocera Voice Server crashes. See **Incoming Mail Settings** on page 179 for information about specifying the Vocera Mailbox Login ID.
Enable Automatic Mailing	n/a	To reduce the time required for troubleshooting, check Enable Automatic Mailing to configure the Vocera Voice Server to email logs automatically to recipient email addresses that you specify.
Select when to email	n/a	Mail all log files sends the most recently closed log file immediately after the server opens a new one; consequently, the system mails a log file at least once a day. For details about when the server closes a log file, see **Working with Server Log Files** on page 173. Mail only when server restarts sends the most recently closed log file immediately after the server restarts; consequently, the system mails only the single log file documenting the cause of the server restart.

Field	Maximum Length	Description
Recipient Addresses	60	Enter the email addresses that will receive the logs in the Recipient Addresses fields. Do not enter more than one address in each field.

To email alerts and log files automatically:

1. Click Email in the navigation bar.
2. Click the Alerts tab to display the Alerts page.
3. Specify the recipient addresses and other settings.
4. Click Save Changes.

Device Management and Reports

This section describes how to manage devices and generate reports.

Device Management

The Devices screen allows you to add, remove, and edit Vocera device information.

You can also search for devices based on a particular field.

About Device Management

Vocera device management features allow you to manage, track, and maintain the hardware devices that connect to the Vocera system.

If your Vocera system includes device management features, you can use them to do the following things:

- Maintain an inventory of Vocera devices
- Increase accountability of organizations that use Vocera devices
- Track Vocera devices through their life cycle
- Prevent loss and control damage to Vocera devices
- Report on the status and usage patterns of Vocera devices

Device Management Guidelines

A proper device management system cannot be implemented without first ensuring that processes have been defined, documented, and approved, administrators and managers have been appointed, and staff have been properly trained and equipped.

Enterprise Guidelines

Identify a staff member for the enterprise that can oversee the Vocera system device management process.

- If your enterprise is large or has multiple sites, there could be multiple Vocera system device managers.

  For a description of system device manager responsibilities, see Device Management Roles on page 186.
- Develop and document device management processes prior to Vocera deployment for the following activities:
  - Device Usage
  - Device Maintenance
  - Inventory Management
  - Device Configuration
  - Device Distribution and Tracking
  - Return Merchandise Authorization (RMA) Process
  - Provision of Spare Devices and Accessories

- Train the system device managers in all device management functionality available in the Vocera Administration Console. Also train on how to administer Vocera Report Server, run scheduled device management and speech recognition reports, which are routed to other administrators and group device managers.

Unit Guidelines

Identify a staff member for each unit deploying Vocera that can oversee the Vocera group device management process.

- For a description of group device manager responsibilities, see Device Management Roles on page 186.
- Develop and document unit processes and policies prior to Vocera deployment for the following activities:
  - Pre-Deployment – includes identifying the best storage location for devices, documenting device repair and return processes, creating a Sign Out/In sheet, and creating daily or shift count.
  - Deployment – includes placing baskets or containers near battery chargers for spare devices and batteries, and regular review of device management.
- Train the group device managers on how to use the Administration Console to edit device information, as well as monitor active devices. Also train on how to view and analyze device management and speech recognition reports.

Managing and Caring for Devices and Accessories

Vocera provides the following items to assist you in managing Vocera devices.

These items can be ordered at vocera.orderprintmaterial.com. The items are free except for shipping costs.

- RMA Device Envelopes
- Badge Repair Kits

Cleaning Vocera Devices and Protective Sleeves

In addition to water and isopropyl alcohol, commercially available germicidal solutions can be used with a damp cloth.

Do not spray the device or immerse it in liquid.

Vocera badges incorporate a silver-ion technology from BioCote® that inhibits the growth of odor-causing bacteria, fungus, and algae.

Providing Attachment Options to Staff

Vocera offers various device attachments.

These are important for the proper use of the devices. They also inhibit users from pocketing devices and accidentally taking them offsite. To control costs and make the staff accountable, the first attachment could be offered free of charge to the staff member, and additional attachments could be stocked in a designated area, such as a Gift Shop, for purchase.

Upgrading from Another Device Inventory System

If your enterprise currently has an inventory system in place to manage Vocera devices, a system administrator should export the data from your current inventory system into CSV format, modify the data so that it conforms to Vocera's Devices template, and then import the data directly into the Vocera database.

For more information on importing devices, see Importing Data from a CSV File on page 162.

Note: System device managers and group device managers do not have privileges to import data into the Vocera system. A system administrator must perform that task.

If you do not have an inventory system in place and Vocera devices have already been deployed to groups or units, the devices will be automatically loaded into the system when they connect to the Vocera Voice Server. You can then generate reports on device usage to determine how the devices should be assigned and fill in any missing information.

Device Management Licensing

If you have a Vocera Enterprise License, Vocera device management features, including Vocera Report Server software and device management reports, are included with your license.

If you have a Vocera Standard License, there is an additional charge for Vocera Report Server software and Device Management. To obtain additional Vocera licenses, please contact Vocera.

Device Management Roles

Learn about the device management roles including a description of each.

The device management features of the Vocera system are available to the following users:

Table 67: Device management roles

Role	Permissions Required	Description
System Administrator	Perform System Administration	Individuals with full permissions for adding, editing, and deleting data in the Administration Console. System administrators must set up system device managers and group device managers, and use Vocera Report Server to schedule device management reports to be generated and e-mailed to users. They can also add, import, export, or update devices. The Perform System Administration permission is needed to be a system administrator. See System Administrators on page 25.
System Device Manager	Perform System Device Management	Individuals with tiered administrator access to the Status Monitor and Devices screens of the Vocera Administration Console, with full permission to add, edit, and delete device data, including device status values, for all sites. The Perform System Device Management permission is needed to be a system device manager. To define which users are system device managers, the system administrator should create a group, for example, "Tiered Admin-Perform System Device Management," grant the group the Perform System Device Management permission, and populate it with members who will be system device managers. See Tiered Administrators on page 26. Sometimes this role is split between two people with one handling inventory and return merchandise authorization (RMA) and the other doing reporting and lost device troubleshooting. Each site may have a Vocera system device manager or a single person may manage Vocera devices for all sites.

Role	Permissions Required	Description
Group Device Manager	none	Individuals who can manage devices owned by groups. Group device managers can access the Status Monitor and Devices screens of the Vocera Administration Console, but they cannot view or modify devices owned by other groups whose devices they do not manage.
		No tiered administrator permissions are needed to be a group device manager. A system administrator defines which users are group device managers by assigning them to a group that manages the devices of another group. See Group Device Managers on page 68.

For a list of device management processes and best practices for system device managers and group device managers, see Device Management Processes on page 217.

System Device Manager Responsibilities

Learn about the responsibilities of a System Device Manager.

Key responsibilities for the system device manager include:

- Receiving Vocera devices into inventory when a new shipment arrives
- Configuring Vocera devices to connect to the wireless network
- Labeling devices
- Mapping device labels to serial number and MAC address
- Assigning devices to group or units
- Troubleshooting problems with devices
- Repairing devices and routing them back to the owning group
- Obtaining return merchandise authorization for non-functioning devices that are under warranty
- Retiring devices that are damaged and are no longer under warranty
- Tracking overall device utilization of the units and groups
- Scheduling device inventory reports to be generated and e-mailed to group device managers
- Ordering new Vocera devices

Group Device Manager Responsibilities

Learn the duties of a Group Manager in the Vocera System.

Key responsibilities for the group device manager include:

- Analyzing reports of device inventory and recognition results by device
- Keeping track of the Vocera devices owned by the group and limiting the number of devices that get lost
- Ensuring that the Vocera devices are in good working condition
- Labeling devices (if not done by System Device Manager)
- Routing devices that need repair to the system device manager
- Maintaining a set of spare devices, batteries, and attachments
- Ensuring that users have the necessary Vocera accessories

Device Management Capabilities per Role

Learn the capabilities of a Device Manager in the Vocera environment.

The following table shows the device management capabilities of system device managers and group device managers:

Table 68: Device management capabilities

Device Management Capability	System Device Manager	Group Device Manager
View the Devices tab	Yes	Yes (for managed groups only)
Add and delete devices	Yes	No
Change the MAC Address, Serial Number, or Tracking Date fields of a device	Yes	No
Modify other device fields that are not read-only.	Yes	Yes
Add, edit, and delete device statuses	Yes	No
Import, export, and update devices	No	No
View the Device Status Monitor	Yes	Yes (for managed groups only)

Important: System device managers and group device managers cannot use the Maintenance screen of the Administration Console to import, export, or update devices. A system administrator must perform those tasks. For more information, see **Performing Server Maintenance** on page 160.

About Serial Numbers and MAC Addresses

Learn about the unique identifiers for Vocera devices and devices used with the Vocera system.

Vocera uniquely identifies devices by the MAC Address field as an alphanumeric value. The Vocera system can derive the MAC address from the serial number, also an alphanumeric value. When you add or update a device and enter the serial number for a Vocera badge, the MAC Address field is populated automatically.

The length of serial numbers varies per device type:

Table 69: Serial Number Length per Device Type

Device Type	Serial Number Length
B3000n	12
B3000	12
B2000	12
Smartphone	10
Cisco Unified Wireless IP Phone 7921G, 7925G, and 7926G	12

Most MAC addresses for Vocera badges have the following 6-character prefix: `0009ef` where the last 6 characters of the MAC address are identical to the last 6 characters of the serial number. Vocera Smartphones have a different MAC address range than Vocera badges.

When you add or update a Vocera badge, Vocera checks for consistency of the serial number with the MAC address. The last 6 characters of the serial number must match the last 6 characters of the MAC address. If you provide a Vocera badge serial number without a MAC address, the system automatically fills in the value, whether you are using the Administration Console to add or update the device or are importing the data from a CSV file.

Using a Barcode Scanner to Add Devices

Vocera devices have labels on the back that include barcodes for the serial number and MAC address of the device.

An inventory sheet with barcodes of the badges' serial numbers is included with every Vocera badge pack. You can use a handheld barcode scanner to scan the badge labels or the inventory sheets. When you scan a Vocera device barcode label using a scanner with keyboard emulation, the data scanned appears at the cursor as if you had typed it from the keyboard. This helps you avoid typographical errors in entering serial numbers and MAC addresses.

Tip: The system device manager should scan new devices into the Vocera system *before* configuring them.

When you receive a shipment of badges from Vocera, it is much easier to scan barcodes for badge serial numbers from the inventory sheet that accompanies the Vocera badge pack. The inventory sheet includes barcodes for the serial numbers of all badges packed in the box.

The following figure shows a user scanning barcodes from a Vocera inventory sheet.

Figure 19: Scanning an inventory sheet

Individual badges are shipped in a plastic clamshell that also has barcode labels. Before opening the clamshell, you can scan the barcodes of the MAC address and serial number from the back of the clamshell.

The following figure shows a user scanning barcodes from the back of a badge clamshell.

Figure 20: Scanning a badge clamshell

The following figure shows a user scanning the barcode label on the back of a Vocera badge.

Figure 21: Scanning a badge

To add devices into the system using a barcode scanner:

1. Make sure your scanner is capable of reading and scanning **Code 128** barcodes. See Barcode Scanner Requirements on page 191.

2. Obtain either the devices or inventory sheets for the devices you need to scan.

3. Log in to the Administration Console.

4. Click Devices in the navigation bar.

5. Click Add New Device. The Add/Edit Device dialog box opens.

6. Enter common values in the Add/Edit Device dialog box that are shared between all devices you are scanning.

   • If the devices share the same Tracking Date, Owner, and Site, specify values for those fields. Otherwise, leave them blank for now and fill them in later.

   • If you are assigning the devices to a group, change the status from "Unregistered" to "Inventory" or "Active."

   • If the devices are shared by multiple users in the group, make sure to check the Shared Device? box.

   > ⚠️ **Important:** These values will be used for all of the devices that you scan during the session.

7. Click the Serial Number field.

8. Using the scanner, scan the serial number from the device or the inventory sheet.

   > ⚠️ **Important:** If you are scanning badge serial numbers, the MAC Address field is automatically populated, its value derived from the serial number.

9. Once the Serial Number and MAC Address fields are completed, the device is saved automatically after a brief pause. The Add/Edit Device dialog box remains open and the Serial Number and MAC Address fields are cleared so that you can add another device.

To search for a device using a barcode scanner:

1. Log in to the Administration Console.

2. Click Devices in the navigation bar.

3. Click the Search By field, and select either "Serial No" or "MAC Address."

4. With the cursor in the Search field, use the scanner to scan the serial number or MAC address label from the device.

5. The matching device is selected in the Devices list. To edit it, click Edit Device.

Tips for Scanning Devices

Learn the guidelines for scanning Vocera badges.

When you scan barcode labels on a Vocera device, follow these guidelines to ensure a good scan:

- Hold the device the typical reading distance from the scanner. The typical reading distance varies depending on your scanner model. For some scanners, the typical reading distance is 0 to 4 inches.
- Hold the device at a 45 degree angle away from the scanner.
- Scan the barcodes from top to bottom. In other words, scan the serial number barcode first and then the MAC address barcode. These are the order of the fields in the Add/Edit Device dialog box. If you scan the MAC address barcode first, the Serial Number field will be populated with the MAC address, and the record will therefore be invalid.
- If you are scanning a Vocera badge, scan only the serial number. The MAC address field is populated automatically.

Barcode Scanner Requirements

To scan Vocera barcodes, you must use a scanner capable of reading and scanning **Code 128** barcodes.

Many scanners are capable of reading and scanning Code 128 barcodes by default. Otherwise, you can configure the scanner to scan such barcodes. For information on how to configure your scanner to read and scan Code 128 barcodes, refer to your scanner's documentation.

When you scan a barcode, many scanners are preconfigured to automatically add a carriage return to move to the next field. If your scanner does not move to the next field, check your scanner documentation for instructions on how to configure the suffix or postamble character.

Automatically Loading Devices into the System

Vocera automatically loads new devices into the system the first time you connect to the Vocera Voice Server.

This feature ensures that every device that connects to the Vocera Voice Server is recorded by the system for inventory purposes.

When the server automatically loads a new device, it records the following device information:

- MAC Address
- Serial Number
- Site
- Type
- Color

By default, the status given to devices automatically loaded by the server is "Unregistered." The system device manager should use the Devices page of the Administration Console to assign unregistered devices to an owning group and change the status from "Unregistered" to "Inventory" or "Active." See Adding or Editing a Device on page 195.

Labeling Devices

When you add a device to the Vocera system, one of the most important fields is the Label field because it uniquely identifies the device by associating it with a group, unit, or user.

The value entered in the Label field should also be the value on the actual label affixed to the front of the device. Labeling the device is important for loss prevention; the label clearly identifies the device and prevents it from being adopted into another department's inventory.

When you label devices, follow these guidelines:

* The Label field that you enter for devices in the Administration Console is limited to 20 characters and the value must be unique. Keep this in mind before you create the physical labels that will be applied to devices.
* Prefix the label text for each device with the abbreviation of the group (for example, RAD for radiology and CICU for cardiac intensive care unit) that owns the device. Other visual cues such as different colored labels, dots, or stickers can help quickly identify the group.
* Labels should be applied directly to the *front* of a B2000 badge for easy identification. You may also want to label the back of the badge.

Figure 22: B2000 badge with a label

* Labels should be applied directly to the *back* of a B3000 badge, beneath the battery compartment.
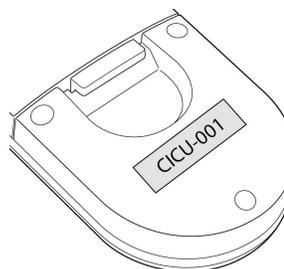
Figure 23: B3000 badge with a label

* Label Vocera Smartphones by placing the label on the ID Label Window located on the battery door.
* **DO NOT use metallic or magnetic labels to label the device.** Metallic or magnetic labels —including labels that use metal-based dye—can adversely affect the device's radio.
* DO NOT apply a label to the protective sleeve.
* If the device is shared between multiple users, the label should have a unique sequential identifier, such as RAD-001, RAD-002, and so on. The sequential numbering of devices makes it easier for the device manager to identify whether a device is missing from the sequence.
* If the device is not shared and you know the user's name, the label could have the user's initials, such as RAD-001-JP.
* If you want to use the same label as a device that has been retired, you must change the Label field for the retired device first. You can prepend the label of the retired device with the string "OLD-" or "RET-".

Monitoring Active Devices

After a device has been added to the system and assigned to a group, system device managers, group device managers, and system administrators can use the Device Status Monitor page of the Administration Console to monitor all active devices on the system.

Devices are listed by group.

For information about using the Device Status Monitor page, see **Device Status Monitor** on page 96.

> **Note:** Unregistered devices, that is, devices that have not yet been recorded by the system device manager and assigned to a group, can be used to log into the Vocera system. However, unregistered devices are not listed in the Device Status Monitor.

Reporting on Devices

The Vocera Report Server provides several asset tracking reports that show which Vocera devices are being used and by which users or departments.

They can help you view device inventory, find missing devices, identify non-functioning devices, and plan for department needs based on usage patterns.

The following table lists device management reports available in Vocera Report Server. For more detailed information about these reports, see the *Vocera Report Server Guide*.

Table 70: Device management reports

Report	Description
Device Last User Access	Displays the last user to log in to a device. This report can be configured to show all devices that have accessed the Vocera system, devices where users have not logged in for several days (lost devices), and devices that users have logged in for the first time ever (unregistered devices) or for the first time in a long time (lost devices that have been found).
Device Last Network Access	Shows when a device last accessed the Vocera Voice Server and what access point or area it was associated with. If a user is not logged in to the device at the last access time, the user is identified as "Not Logged In." Otherwise, the actual user name is displayed. Devices are grouped by the owning group. Each device's data spans two rows to accommodate all of the information.
Device Inventory - Summary	Summarizes which devices each department is using. Information is grouped by department, and within each department, by device MAC address. To see who in that department is using the device, use the detailed version of the report.
Device Inventory - Detail	Shows details about which devices each user in each department is using. Information is grouped by department, and within each department, by device MAC address.
Device Usage Report	Shows which devices each user in each department is using. This report helps identify devices that have moved to a different department and devices that may not be working properly (based on short periods of use).
Device Status Tracking	Shows the device status changes that occurred for each device. This report helps identify which devices are currently at a particular status (such as Lost, In Repair, or RMA'ed).

Managing Devices

This section describes various concepts and tasks associated with managing Vocera Devices.

Viewing Devices

Use the Devices screen to perform device management tasks.

When you click Devices in the navigation bar, you can view devices currently in the Vocera system. System administrators and system device managers can view all devices. Group device managers can view only devices owned by groups whose devices they are permitted to manage.
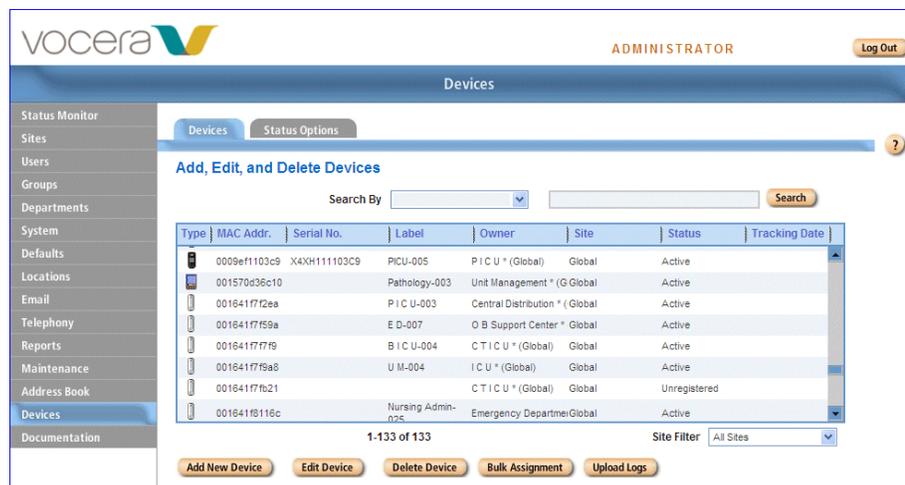
Figure 24: Devices screen

Finding Devices

You can search for a device by MAC address, serial number, label, owning group, device status, or tracking date.

Finding a device is easy. As you type a value in the Search field, matching devices are listed. You can select a value from the drop-down list, or type the complete value and click Search to locate it.

Sorting Devices

You can sort the Devices table by any of the columns.

For example, to sort by serial number, click the Serial No. column heading. You can sort by only one column at a time.

Filtering Devices by Site

To filter the Devices table by site, select a site in the Site Filter list below the table.

By default, devices are listed for all sites.

Device Icons

Review the icons representing the available devices in the Vocera system.

The Devices screen displays the following icons to identify different types of Vocera devices:

Table 71: Device icons

Icon	Device Type
	B3000n
	B3000

Icon	Device Type
	B2000
	Vocera Smartphone
	Cisco Unified Wireless IP Phone (7900 series)
	Motorola MC70

Adding or Editing a Device

As soon as a Vocera device arrives at a site, its identifying information should be entered into the Vocera system so that it can be tracked and monitored appropriately.

This should be done even before the device is configured. This helps prevent the device from being lost or transferred to another department. It also allows you to monitor and report on the device status.

There are three ways devices can be added to the Vocera system:

* Automatically load devices when they connect to the Vocera Voice Server. See **Automatically Loading Devices into the System** on page 191.
* A system administrator can import devices from a CSV file. See **Importing Data from a CSV File** on page 162.
* A system administrator or system device manager can add devices using the Devices screen in the Administration Console.

> **Note:** Group device managers cannot use the Administration Console to add devices.

To add or edit device information using the Devices ***screen:***

1. Click Devices in the navigation bar.
2. Click Add New Device to add information for a new device, or choose a device from the list and click Edit Device to edit information for an existing device.

   The Search option can help you find devices quickly. In the Search By list, select a field to search, and then type a value in text field and click Search. As you type a search value, the field displays a drop-down list of closest matching values.
3. The Add/Edit Device dialog box opens. Add or edit data as appropriate.

   To ensure the accuracy of serial numbers and MAC addresses, you can use a barcode scanner to scan device labels or inventory sheets. For more information, see **Using a Barcode Scanner to Add Devices** on page 188.
4. After working with a page in the dialog box, do one of the following:
   * Click Save to save changes, close the Add/Edit Device dialog box, and display the Devices page.
   * Click Save & Continue to save the device information and leave the Add/Edit Device dialog box open to add information for another device.

Device Information

The Device Information page of the Add/Edit Device dialog box (or the corresponding fields in the data-loading template) lets you specify the information for a device, such as the serial number, MAC address, color, type, status, site, whether the device is shared, and other information.

Table 72: Device information fields

Field	Maximum Length	Description
Serial Number	15	Specify the serial number of the device. For Vocera badges, the serial number is 12 characters. For Vocera Smartphones, the serial number is 10 characters.
Color	n/a	This read-only field specifies the color of the device, which is determined from the serial number. Vocera badges can be white or black.
MAC Address	12	For Vocera badges, this field is automatically populated when you enter a valid value in the Serial Number field; the last 6 digits of the serial number and the MAC address are identical. For Vocera Smartphones, remove the battery door and then the battery, and then enter the MAC address and serial number listed on the back of the phone. Note: To delete the MAC address for a Vocera badge, you must first delete the serial number.
Type	n/a	This read-only field specifies the type of device, which is determined from the serial number. Device types include B3000n, B3000, B2000, Smartphone, Apple, Android, and MC70.
Label	20	A label that uniquely identifies the device. For more information, see Labeling Devices on page 191.
Owner	50	Specify the group that owns the device. In the Add/Edit Device dialog box, click the Select button to open the Select Group dialog box, then choose a group from the list and click Finish. The site of the group that owns the device can be different from the site of the device itself.
Tracking Date	n/a	A date used to track the device, for example, the date it was sent for repair or RMA'ed. Select a tracking date by clicking the calendar icon to the right of the field, or type the date in the field. If you type the date, use the correct date format: United States: `mm/dd/yyyy` Other locales: `dd/mm/yyyy`
Site	50	Specify the device's home site. In the Add/Edit Device dialog box, click the Select button to open the Select Site dialog box, then choose a name from the list and click Finish. • If your organization has multiple sites connected to the same Vocera Voice Server, choose the home site that represents the device's physical location. • If your organization does not have multiple sites, accept the default Global setting. When working in the data-loading template, leave this field blank to accept Global.
Status	20	Select the device status from the list. If you have System Administrator permission, you can add new statuses on the Status Options tab and delete statuses.
Shared Device?	n/a	Check this box to indicate that the device is shared by multiple users.
Disable Device?	n/a	Check this box to disable the device. If the device is disabled and the Call button is pressed, the following prompt is played, "This device has been disabled, please contact your administrator". The user upon hearing the prompt will return the device preventing inventory loss. **Note:** When you disable a device, if a user is logged into the device, they'll be logged out immediately.
Notes	1000	A multi-line text box that lets you provide further information about the device status, for example, "Badge stopped working on [DATE] after accidentally being immersed in water" or "Badge sent to IT to repair the battery latch."

Device Status

The Device Status page of the Add/Edit Device dialog box displays status information about the device, such as the current logged in user, location, and local site, as well as the IP address of the device and whether it is currently in a charger.

All of the fields are read-only. This information is similar to the status information you will see in the Device Status Monitor. For more information, see **Device Status Monitor** on page 96.

Table 73: Device status fields

Field	Description
User	Shows the name of the logged in user. If a user is not logged into the device, the field displays "Not Logged In."
Location	Shows the name of the location of the access point to which the device is currently connected. If a location name was not assigned, the field shows the access point's MAC address.
Local Site	Shows the name of the physical site the user is associated with.
IP Address	Shows the network address of the device. If the network address is assigned dynamically through the DHCP server, the IP address can change as the device moves between access points.
In Charger	Indicates whether the device is currently in a battery charger.

Deleting Devices

The Vocera Voice Server allows you to delete devices that have been entered into the system with the wrong serial number or MAC address.

Only system administrators and system device managers can delete devices. The deletion takes effect immediately.

> **Tip:** Do not delete an inactive device. When a device is no longer in use, *retire* it from the system instead of *deleting* it. If you delete a device that has appeared on the network at any previous time, it will continue to appear in device management reports.

Do not delete an active device. If you delete a device that is still in use, it will automatically be added again to the system the next time it connects to the server.

To delete a device:

1. Click Devices in the navigation bar to display the Add, Edit, and Delete Devices page.
2. Select one or more devices to delete.

   To select two or more adjacent rows on the Devices tab, click the first row, then hold down SHIFT while you click the last row to select.

   To select two or more nonadjacent rows on the Devices tab, click the first row, then hold down CTRL while you click other rows to select.

   The Search option can help you find devices quickly. In the Search By list, select a field to search, and then type a value in the Search field. As you type, a drop-down list appears with up to 10 matching names. Select one, or click Search to go to the first match.
3. Click Delete Device.

Bulk Device Assignment

The Bulk Device Assignment dialog box lets you assign status, owner, tracking date, and site values to multiple devices at a time.

This feature is helpful if you are processing a group of devices at once. For example, you may be assigning several devices to a group, or you may be changing the status of devices to "RMA'ed".

To assign status, owner, and site values to multiple devices:

1. Click Devices in the navigation bar to display the Add, Edit, and Delete Devices page.

DEVICE MANAGEMENT

2. Optionally, sort the Devices table by one of the columns.

3. Select one or more devices.

   To select two or more adjacent rows on the Devices tab, click the first row, then hold down SHIFT while you click the last row to select.

   To select two or more nonadjacent rows on the Devices tab, click the first row, then hold down CTRL while you click other rows to select.

4. Click Bulk Assignment.

5. The Bulk Device Assignment dialog box opens.

   To add more devices to the devices list, use the Search By field to search for devices by MAC Address or Serial No. After selecting MAC Address or Serial No, type the search value. As you type a search value, the field displays a drop-down list of closest matching values. You can select a value from the drop-down list, or type the complete value and click Add. The matching device appears in the devices list.

6. In the Assignment box, specify the Status, Owner, Tracking Date, and Site values to assign to the devices in the device list.

7. Click Save to save changes, close the Bulk Device Assignment dialog box, and display the Devices page.

Table 74: Bulk device assignment fields

Field	Maximum Length	Description
Status	20	Select the device status from the list. On the Status Options tab, you can define additional device status values.
Owner	50	Use the Owner field to specify the group that owns the device. In the Bulk Device Assignment dialog box, click the Select button to open the Select Group dialog box, then choose a group from the list and click Finish.
Tracking Date	n/a	Select a date used to track the device, for example, the date it was sent for repair or RMA'ed. If you type the date, use the correct date format: United States: `mm/dd/yyyy` Other locales: `dd/mm/yyyy`
Site	50	Use the Site field to specify the device's home site. In the Bulk Device Assignment dialog box, click the Select button to open the Select Site dialog box, then choose a name from the list and click Finish. • If your organization has multiple sites connected to the same Vocera Voice Server, choose the home site that represents the user's physical location. • If your organization does not have multiple sites, accept the default Global setting. When working in the data-loading template, leave this field blank to accept Global.

Uploading Badge Logs

You can select a currently connected badge on the Devices page, and then click the Upload Logs button to upload the badge's logs to the Vocera Voice Server.

Uploading the Badge log through the Administration Console is more convenient than using the badge's configuration menus to upload logs.

When you upload badge logs, the files are assembled into a single `.tar.gz` file in the `\vocera\logs\BadgeLogCollector\uploads` directory on the Vocera Voice Server. The format of the filename is `DATETIME-USERNAME-BADGEMAC-udd.tar.gz`.

To upload badge logs:

1. Click Devices in the navigation bar to display the Add, Edit, and Delete Devices page.
2. Click to select the Vocera device. Select only device at a time.

> **Note:** The badge you select must be currently connected to the Vocera Voice Server.

3. Click Upload Logs.
4. Click OK.

Adding, Editing, and Deleting Device Status Values

Learn about the status values for Vocera devices.

The following table lists the default status values for devices:

Table 75: Default devices statuses

Status	Description
Unregistered	Device was auto-loaded by Vocera Voice Server and the status has not been updated by the System Device Manager. **Note:** This status value cannot be deleted or modified.
Active	Device has been assigned to a Group Device Manager to deploy.
Inventory	Device is in inventory but has not been deployed.
Lost	Device has been lost.
Pending RMA	System Device Manager has requested an RMA for the device from Vocera.
Received for Repair	System Device Manager has received the Vocera device for diagnosis and repair.
Retired	Device is no longer in use.
RMA'ed	System Device Manager has shipped Vocera the device for repair or replacement.
Sent for Repair	Group Device Manager has followed the process to report device as defective.
Spare	Device has been assigned to a Group Device Manager and is being used as a spare.

You can define any number of other status values based on the device management processes you have implemented. On the Status Options tab, you can add, edit, and delete device status values. You can also change the order of device status values.

> **Note:** Only system administrators and system device managers can add, edit, and delete device status values.

To add a device status value:

1. Click Devices in the navigation bar to display the Add, Edit, and Delete Devices page.
2. Click the Status Options tab to display the Add, Edit and Delete Device Status page.
3. Click Add.
   The Add New Device Status dialog box opens.
4. In the Device Status field, enter a new device status.
5. In the Description field, enter a description of the status (up to 100 characters).
6. Do one of the following:
   - Click Save to save changes, close the Add New Device Status dialog box, and display the Add, Edit and Delete Device Status page.

- Click Save & Continue to save the device information and leave the Add New Device Status dialog box open to add information for another device.

To edit a device status value:

1. Click Devices in the navigation bar to display the Add, Edit, and Delete Devices page.
2. Click the Status Options tab to display the Add, Edit and Delete Device Status page.
3. Select a value in the Device Status Options list.
4. Click Edit.

   The Edit Device Status dialog box opens.
5. In the Device Status field, edit the device status.
6. In the Description field, edit the description of the status (up to 100 characters).
7. After editing the device status, click Save to save changes, close the Edit Device Status dialog box, and display the Add, Edit and Delete Device Status page.

To reorder device status values:

1. Click Devices in the navigation bar to display the Add, Edit, and Delete Devices page.
2. Click the Status Options tab to display the Add, Edit and Delete Device Status page.
3. Select a value in the Device Status Options list.
4. Click Move Up or Move Down to move the status value up or down.

> **Note:** You cannot change the first status value, which is "Unregistered".

To delete a device status value:

1. Click Devices in the navigation bar to display the Add, Edit, and Delete Devices page.
2. Click the Status Options tab to display the Add, Edit and Delete Device Status page.
3. Select a value in the Device Status Options list.
4. Click Delete.
5. Click OK to confirm that you want to delete the status value.

   The Replace Device Status dialog box opens.
6. In the Device Status list, select a device status to replace the status you deleted.
7. Click Save to save changes, close the Replace Device Status dialog box, and display the Add, Edit and Delete Device Status page.

Add/Edit/Replace Device Status

The Add/Edit Device Status dialog box lets you add and edit device statuses.

To display this dialog box from the Status Options page, click Add or Edit.

Field	Maximum Length	Description
Device Status	20	If you are adding or editing a device status, type the name of the status.
Description	100	Enter a brief description of the device status, indicating what the status means and who has the device.

Replace Device Status

The Replace Device Status dialog box lets you replace a device status you are deleting with another status.

To display this dialog box from the Status Options page, select a status and click Delete.

Field	Description
Device Status	Select a device status from the list.

Managing Shared Devices

To reduce the total cost of hardware, Vocera devices are often shared between multiple users rather than being assigned to a single user.

In a shared device model, it's important to track inventory frequently and to make sure the equipment is functioning properly. If you use a shared device model, follow these guidelines:

- Make sure the Shared Device? box is checked when you add each device into the Vocera system.
- Make sure the label on a shared device indicates the owning group or unit instead of an individual user.
- To track shared devices and make sure they have not been lost, use the **Device Last User Access** or **Device Last Network Access** reports.

Generating Reports

Use the Reports screen to generate lists of users, groups, and address book entries that you can display online or print.

You can choose from the following report types:

Table 76: Administration Console reports

Report type	Description
User Summary	Lists all registered users for the selected site, and includes Alternate Spoken Names and Desk Phone fields for each user. If you select All Sites, users are sorted by site.
Temporary User Summary	Lists all temporary users for the selected site, and includes Site, Desk Phone, Dynamic Extension, and Expiration Date fields for each user. If you select All Sites, users are sorted by site.
Vocera Access Anywhere Users	Lists the users for the selected site that have Vocera Access Anywhere enabled.
Group Detail	Lists all groups for the selected site, and enumerates the members of each. If you select All Sites, groups are sorted by site.
Group Nesting	Lists groups for the selected site that have other groups contained inside them. Groups without nested groups are excluded. If you select All Sites, groups are sorted by site.
Call Flow	Lists the forwarding chain, the call scheduling type (Sequential or Round Robin), and the call flow for groups in the selected site.
Address Book	Lists the names, site, identifying phrase, phone number, and pager number of every entry in your address book.
Site	Lists the groups and locations for every site on the system.

To generate a report:

1. Click Reports in the navigation bar to display the Reports page.
2. In the Select Site list, select a site to use for the report. The default is All Sites.

   Note: The Site report shows all sites regardless of site selected in the Select Site list.

3. Choose a report type.
4. Click Generate to generate the report and display it in the console.
5. Click Printable Format to display a printable version of the report in a new window.
6. Choose File > Print from the menu at the top of the new window to print the report.

Speech Recognition

This part of the manual describes Vocera features and settings that control speech recognition.

These include:

- Techniques that administrators can use to resolve speech recognition problems.
- How to provide a custom Help prompt for users.

- Troubleshooting Speech Recognition on page 204
- Providing a Custom Help Prompt on page 214

Troubleshooting Speech Recognition

This appendix explains the basics of the system grammar and describes techniques for resolving speech recognition problems.

About Speech Recognition

When a user issues a verbal command to the Genie or responds to a question the Genie asks, Vocera attempts to process the utterance by finding a match in the *recognition space*.

The recognition space has the following components:

- *A static grammar*, which includes commands such as "Call" and "Broadcast" as well as possible responses such as "Yes" and "No", digits such as "One" and "Two", and so forth. The static grammar is installed by Vocera and cannot be changed by a customer.
- *A dynamic grammar*, which includes all the spoken names a user can possibly utter. The dynamic grammar includes the names of users, groups, sites, locations, address book entries, and all their possible alternates, such as spellings of user names and the singular and plural names of groups.

  Each site has its own dynamic grammar. It is completely determined by values that you enter in the database.
- *A personal grammar*, which includes the buddies of an individual user, as well as any personal learned names, and learned commands.

  Each user has his or her own personal grammar.

The recognition space varies according to the user issuing the command and the site the user is calling. That is, because each site has its own grammar, and each user has a personal grammar, the actual recognition space is likely to be slightly different for any individual making a call.

The Dynamic Grammar

The dynamic grammar is the largest component of the recognition space.

It is always considerably larger than the total number of users, groups, sites, locations, and address book entries, because it also includes all the possible *alternates*. In some situations, you explicitly add alternate names yourself, such as when you enter the plural name of a group. In other cases, the system itself automatically adds them, such as the spellings of a user name.

For example, each user you enter in the system adds a *minimum* of four spoken names to the dynamic grammar, and possibly as many as thirteen names, as follows:

- The user name itself (Call *Patrick Curtis*)
- The spelling of the user's first name (Call *P-A-T-R-I-C-K*)
- The spelling of the user's last name (Call *C-U-R-T-I-S*)
- The spelling of the user's combined first and last names (Call *P-A-T-R-I-C-K-C-U-R-T-I-S*)
- The first name, last name, and department, if the associated field on the System|Preferences page is selected (Call *Patrick Curtis in Managers*)

- The first name and department, if the associated field on the System|Preferences page is selected (Call *Patrick in Managers*)
- The three alternate spoken names on the Speech Recognition page of the Add/Edit User dialog, if specified (Call *Pat Curtis*)
- The spellings of each of the alternate spoken names, if specified (Call *P-A-T-C-U-R-T-I-S*)
- The identifying phrase on the Speech Recognition page of the Add/Edit User dialog, if specified (Call *Patrick Curtis in the basement*)

Similarly, groups, sites, locations, and address book entries can all potentially have alternate names. The following table summarizes the impact of each database entry on the recognition space:

Table 77: Spoken names for dynamic grammar entries

Database Entry	Minimum Spoken Names	Maximum Spoken Names
Empty System	12	N/A
User	4	13
Group	3	6
Site	8	9
Location	2	4
Address Book Entry (Person)	4	11
Address Book Entry (Place)	2	9

Site Grammars

Partitioning a deployment into sites improves speech recognition, because each site has its own dynamic grammar, which is the largest component of the recognition space.

When a badge user speaks a command, Vocera attempts to process it by combining the dynamic grammar of a single site with several smaller grammars. Specifically, Vocera searches the following grammars while processing a badge user utterance:

- Either of the following dynamic grammars:
  - The dynamic grammar of the caller's current site
  - The dynamic grammar of the site the caller explicitly connects to
- The Global site grammar
- The static grammar
- The badge user's personal grammar

Note: See **About Speech Recognition** on page 204 for more information on partitioning a deployment into sites.

Vocera always includes the static grammar, the grammar of the Global site, and the badge user's personal grammar while processing voice commands. However, Vocera includes the dynamic grammar of only a single site, not the grammars of every site, while processing the command.

For example, suppose the Central Pacific Resort deployment has two sites—Carmel and Monterey—in addition to the Global site. If a badge user in Carmel issues the command, "Call Adda Turner", Vocera uses the following grammars to process it:
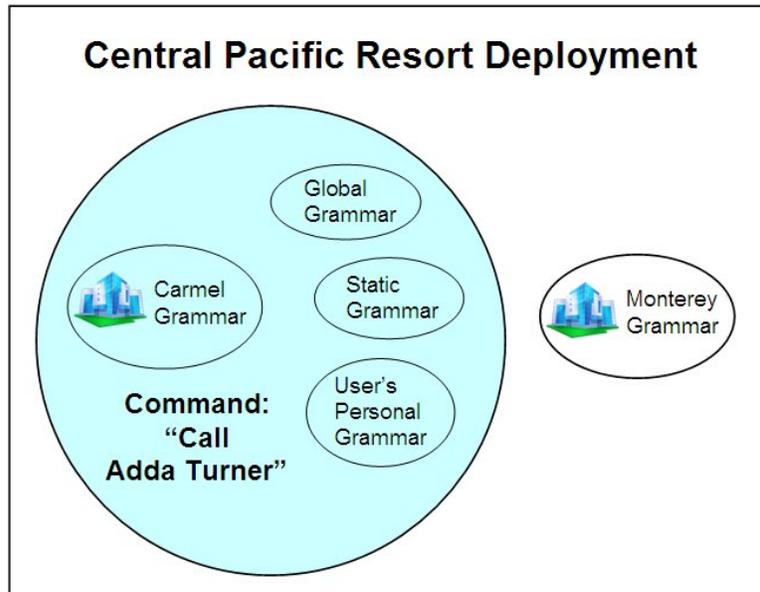
Figure 25: Grammars used at the Carmel site

Contacting a badge user at a *remote* site is a two-step process. For example, suppose the Carmel user in the previous example wants to call Adda Turner, but Adda's home site is Monterey. The user needs to speak two commands to place this call:

1. Connect to Monterey.
2. Call Adda Turner.

Vocera searches the dynamic grammar of the Carmel site—the current site of the user placing the call—to process the first command. After receiving the "Connect to" command, however, Vocera searches the dynamic grammar of the Monterey site, as shown in the following illustration:
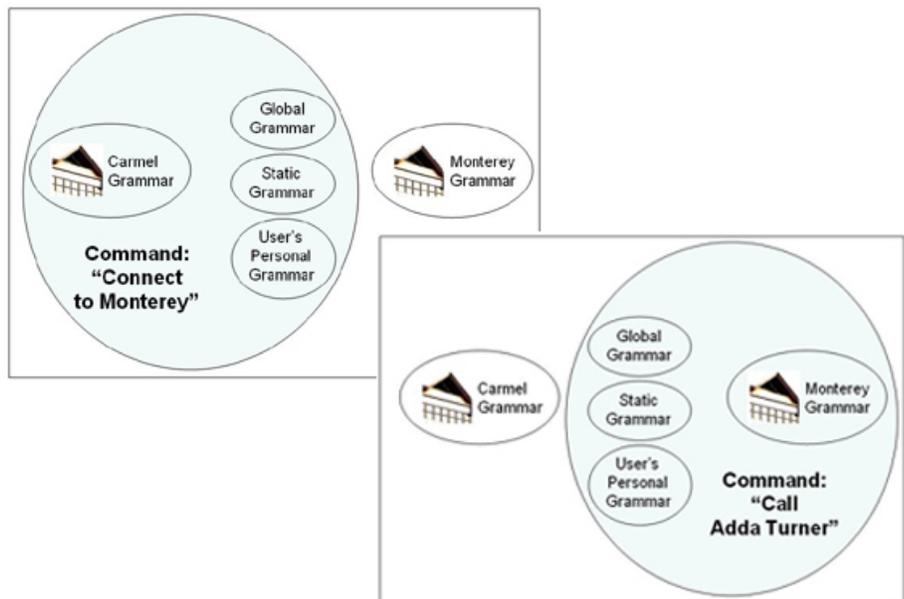
Figure 26: Grammars used after connecting to the Monterey site

When a person places a *telephone call* to the hunt group number or the DID number of the Vocera system, the telephony Genie prompts the caller to say the name of the person or group, or enter an extension. Vocera processes the caller's response to the telephony Genie as follows:

- If the site is not sharing a telephony server, Vocera searches the Global site grammar and the grammar of the telephony server's site.
- If the site is sharing a telephony server and the caller *spoke* a response, Vocera searches the combined grammars of the Global site and any sites associated with the line that the call arrived on.
- If the site is sharing a telephony server and the caller *entered a touch-tone* response, Vocera searches the combined databases of the Global site and every site that shares the telephony server.

See the *Vocera Voice Server Telephony Configuration Guide* and **Working with Multiple Sites** on page 33 for additional information.

Spoken Name Count

The *spoken name count* is the total number of items in the dynamic grammar.

Vocera displays the following spoken name counts:

- The spoken name count for a *site* is the total number of names in the dynamic grammar of that site. This count appears in the Spoken Name Count field on the Add/Edit Site page.
- The spoken name count for the *system* is the total number of names in the dynamic grammars of all the sites in the system. This count appears in the Spoken Name Count field on the System|License Info page.

Because the dynamic grammar is both the largest component of the recognition space and also the component administrators can control, it is important to monitor the spoken name count. As the spoken name count grows:

- The load on the system increases. A large recognition space requires greater processing power to search efficiently.
- The likelihood of mis-recognized speech increases. A large recognition space is more likely to contain similar sounding names.

Using Departments to Improve Speech Recognition

A *department group*, also called a *department*, is a group that corresponds to a department within the organization using the Vocera system.

Departments are a convenient way to let badge users contact each other with voice commands. When a caller specifies a department in a voice command, Vocera can:

- Differentiate among users with the same first and last names.
  For example, if your organization has two individuals named John Smith, a user can issue the voice command "Call John Smith in Tech Support."
- Identify a badge user when the caller knows the first name and department, but not the last name, of other people in the organization.
  For example, a caller can issue the voice command "Call John in Tech Support."

Using Alternate Spoken Names

Use the Alternate Spoken Names field to provide alternative names, phonetic spellings, or additional identifying information so the speech recognition software can recognize variations of a name.

When a user asks the Genie to contact a person or place in the address book ("Call Poison Control"), the speech recognition software in Vocera tries to match the spoken name to a name in a user profile or an address book entry.

People may not always use the name that you entered, however, or they may pronounce it in a way that the Vocera system does not recognize. For example, you may identify an address book entry as "Easton Medical Clinic," but users may refer to it as "The medical clinic."

Several pages in the Administration Console provide fields where you can enter data that can help you prevent speech recognition problems in these situations. For example, when you add or edit a user profile or an address book entry, you can enter data in the Alternate Spoken Names and Identifying Phrase fields.

Guidelines for Alternate Spoken Names

Use the Alternate Spoken Names field to provide alternative names, phonetic spellings, or additional identifying information so the speech recognition software can recognize variations of a name.

When entering an alternative spoken name for a user in the Administration Console, use the following guidelines for the best result.

- If users refer to a person or place in various ways, enter each variation in a different field.

  For example, enter *Bob Jones* and *Rob Jones* in addition to *Robert Jones*. Similarly, enter a nickname that the person or place is known by, such as *Skip Jones*.

  The names you provide must start with a letter or digit. They must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed.

  Note: Even though the characters listed above are allowed, it is unlikely that an alternate spoken name would need underscores (_), or dashes (-).

- **Important:** It is recommended that you do not create an alternate spoken name that contain numeric digits only. For example, a staff ID with numbers and no letters:

  `567748`

  Entering numeric staff IDs is permitted. However, the possible results of using numeric values only is:
  - Slower Genie response time
  - Problems with phone number recognition

- If people use an acronym or initials to refer to an address book entry, provide them as a series of letters separated by spaces.

  For example, if users refer to Easton Medical Clinic as EMC, enter *E M C*. Similarly, enter *A C Hoyle* for A.C. Hoyle.

- If a name has an unusual or confusing pronunciation, enter a name that is spelled as it is pronounced.

  For example, if the system does not recognize the name *Jodie Dougherty*, you could enter *Jodie Dockerty*.

- If users refer to a person by his or her title, provide the full spelling of the title.

  For example, enter *Doctor Shostak* instead of *Dr. Shostak*.

Identifying Phrase Fields

Use the **Identifying Phrase** field to enter a description that distinguishes a person or place from another whose name is spelled the same.

For example, if there are two users named Mary Hill on the system, but one is on the third floor and the other is on the first floor, you might enter *Mary Hill in the Main Cafeteria* as the Identifying Phrase for one user and *Mary Hill in the North Wing Cafeteria* for the other.

As a result, when callers ask for Mary Hill, the Genie prompts them, "Do you mean Mary Hill in the Main Cafeteria?" If the caller says "no," the Genie then prompts, "Do you mean Mary Hill in the North Wing Cafeteria?"

Vocera can also use departments to differentiate among users with the same names. Departments are usually easier to set up and use than identifying phrases, but are applicable only if the users belong to different departments.

Homonym Recognition

The Vocera Genie can only recognize words and phrases that it is specifically trained to recognize. As such, similar sounding names may not be recognized by the Genie.

In version 4.x, the Vocera Voice Server prompts a caller to disambiguate between multiple users whose names are spelled the same way; for example, when two users are named Chris Jenkins, the system uses an identifying phrase (when available) to prompt the caller: "Do you mean Chris Jenkins in 4 West Nursing? Do you mean Chris Jenkins in Imaging?"

Starting with the 5.0 release, the Vocera Voice Server additionally prompts callers to disambiguate between multiple users whose names are pronounced the same way but spelled differently; for example, users named Chris Jenkins and Kris Jenkins.

> **Important:** You must associate identifying phrases or departments with users whose names are spelled or pronounced the same way. The system will play back recorded names, if they are available, to help the caller disambiguate; however, identifying phrases or departments provide better disambiguation options.

Side-Speech Tolerance

Starting with the 5.0 release, the Vocera Voice Server has improved the capability to distinguish a command in a stream of conversation; for example, when the person initiating a call is completing a conversation with another person at the same time.

In this situation, the software will wait until a legal command is spoken, discard the preceding and following speech, and then process the command for recognition.

Buttons-Only Answering

Vocera allows users to accept and reject calls with either voice commands or buttons.

In some situations, background noise can cause poor speech recognition, resulting in the Genie repeatedly saying "I'm sorry, I didn't understand". In other situations, background noise can cause the Genie to prematurely accept or reject calls without user input.

In high-noise environments, you can optionally require users to accept and reject incoming calls by pressing the Call or DND/Hold button. To specify this option, check the Accept Calls Using Button Only setting on the Defaults|Miscellaneous page of the Administration Console. Selecting this feature disables the use of "Yes" and "No" voice commands to accept and reject incoming calls.

By default, this feature is disabled. Enabling it establishes a new system-wide default and may require re-training. Users can optionally override this default, if you allow it. See **Setting System Defaults** on page 118.

Utterance Recordings

Vocera automatically records the spoken utterances of individuals when they interact with the Genie.

You can use these recorded utterances to help identify and resolve speech recognition problems.

Vocera records utterances during the following Genie interactions:

*   Interactions that logged-in users have with the Genie.
*   Interactions that users have with the Genie while trying to log in.

- Interactions that telephone callers have with the hunt-group Genie.

> **Important:** Vocera records *only* the utterances individuals make while interacting with the Genie, *not* the utterances they make during personal interactions with other individuals.

Vocera creates a directory named `\vocera\nuance\callLogs\MyApp` at the root of the drive where the Vocera Voice Server is installed. The system then records utterances and log files within this structure.

The directory tree within `MyApp\` is `[Year]\[Month]\[Day]\[Hour]`. For example, the directory `\vocera\nuance\callLogs\MyApp\2014\07July\17\20` contains utterances recorded on 17 July 2014, between 8:00 and 9:00 pm.

Each directory contains `.wav` files for the user utterances and a log file. The log file contains information that Vocera can use to troubleshoot problems. The `.wav` files frequently contain information you can use to troubleshoot speech recognition problems yourself.

This directory structure contains a set of files that are named similar to the following:

```
NUAN-26-24-VS-209-VM-W2012-deb948cafef0b922ab2287bacf762a9b@10.98.2.209-
Manfred_Morgan-LOG NUAN-26-24-VS-209-VM-W2012-
deb948cafef0b922ab2287bacf762a9b@10.98.2.209-
Manfred_Morgan-utt001-POSTEP.wav NUAN-26-24-VS-209-VM-
W2012-deb948cafef0b922ab2287bacf762a9b@10.98.2.209-
Manfred_Morgan-utt002-POSTEP.wav NUAN-26-24-VS-209-VM-W2012-
deb948cafef0b922ab2287bacf762a9b@10.98.2.209-Manfred_Morgan-utt003-
POSTEP.wav
```

The file name of the log and utterance contains the following information to help you identify the call:

Table 78: Call log filename fragments

Filename Fragment	Description
`NUAN-26-24`	The speech port identifier, internal to Nuance.
`VS-209-VM-W2012`	The DNS name of the server.
`deb948cafef0b922ab2287bacf762a9b`	The SIP session ID for the MRCP channel.
`10.98.2.209`	The IP address of the server.
`Manfred_Morgan`	The name of the user. If a filename does not include a user name, it is an utterance that was recorded during a login attampt.
`LOG`	An identifier indicating that the file contains a Nuance recognition log.
`utt001, utt002, utt003`	Sequentially numbered identifiers for each utterance in the session.
`POSTEP`	An identifier indicating that the utterance has been end-pointed (internal to Vocera).

> **Note:** The system maintains a maximum of 14 days of utterances in the `\vocera\nuance\callLogs\MyApp\` directory.

Recording Badge User Utterances

Vocera records all the utterances users make during Genie interactions and saves them as audio files in the `.wav` format.

You can then listen to the `.wav` files to determine the problems specific users have, such as speaking the wrong forms of commands, mispronouncing user and group names, holding the badge while speaking, and so on.

Here are some problems you can typically resolve by listening to the `.wav` files in the Genie utterance subdirectories:

Table 79: Troubleshooting recorded utterances of badge users

Symptom	Possible Cause	Solution
You hear puffing, breathing, or distorted sounds while user is speaking.	The badge is too close to the user's mouth, possibly because the user is holding it instead of wearing it.	Make sure the user wears the badge with an attachment that keeps it 6-8 inches from the chin.
You hear muffled sounding speech.	The user is holding the badge and covering the microphone.	Make sure the user wears the badge with an attachment that keeps it 6-8 inches from the chin.
You hear distant sounding speech.	The badge is too far away from the user's mouth.	Make sure the user wears the badge with an attachment that keeps it 6-8 inches from the chin.
You hear incorrect forms of commands or keywords that Vocera does not recognize.	The user does not remember the exact form of the command.	Retrain the user with the correct commands. Distribute supplementary learning material, such as the *Vocera Badge User Guide*, the *Vocera Quick Reference Guide*, or the *Vocera Command Poster*.
You hear incorrect user and group names.	The user does not remember or know the exact name of the person he or she is calling.	Show the user how to call other users with the first name and department. See **About Groups and Departments** on page 70 for information about creating departments. See the section called "Calling with Department Names" in the *Vocera Badge User Guide*.
You hear mispronounced user and group names.	The user cannot say the exact name of the user or group accurately, or the user has an accent that Vocera cannot understand.	Show the user how to train the Genie to recognize his or her own voice. See the section called "Training the Genie" in the *Vocera Badge User Guide*.
You hear very rapid speech or unusual pauses in the utterances.	The user has forgotten introductory badge training or has not received it.	Retrain the user. Remind the user to speak clearly and with an even cadence for optimal speech recognition.
You hear clipped words at the beginning of a command or reply.	The user starts issuing a command or replying before the Genie is finished speaking.	Retrain the user. Remind the user to wait for the Genie to finish speaking before replying. When the Genie is speaking, the badge is transmitting. If the user interrupts the Genie, the badge is not yet ready to receive, and the beginning of the user utterance is clipped.
You hear talking after the command or reply is finished.	The user is not pausing at the end of a command or reply, but is possibly trying to speak before the badge connection has been established, or speaking to someone in a conversation unrelated to the badge command.	Retrain the user. Remind the user to pause briefly after issuing a command or reply. The Genie uses a pause at the end of a command or reply as a cue that the command is complete. Continuing to speak effectively creates a lengthy command that the Genie cannot interpret.

Symptom	Possible Cause	Solution
You hear dropouts or choppy sounding voice.	Network problems.	Make sure the access point coverage is adequate for voice in the location where the problem occurred. Make sure the DTIM value of access points on the badge subnet is set to 1. See the *Vocera Infrastructure Planning Guide*.

Recording Telephone System Utterances

Telephone callers outside the Vocera system can place calls to user's badges by dialing the Vocera hunt group number (in an analog telephony integration) or DID number (in a digital telephony integration).

These callers hear the Genie prompt, "Say the full name of the person or group you want to reach or enter an extension."

Here are some problems specific to telephony that you can typically resolve by listening to the `.wav` files in the Genie utterance subdirectories:

Table 80: Troubleshooting recorded utterances of phone users

Symptom	Possible Cause	Solution
You hear dropouts in the utterances.	Network problems between the Telephony server and the Vocera Voice Server, if they are running on separate computers.	Work with the IT administrator to confirm the network connection is functioning properly.
You hear static or distortion.	The trunk line coming into the PBX from outside has problems.	If you hear static or distortion on all calls coming into the PBX from outside—not just calls into the hunt group or DID number—you may be experiencing problems in the trunk line. Notify the PBX administrator of the situation.
You hear distant sounding speech.	A speaker phone is too far away from the caller or a cell phone is breaking up. An inadequate volume level is set in the PBX.	If you notice low levels on only some outside calls, the phones placing these calls may be at fault. If specific callers regularly have these problems, suggest that they call in from a different phone. If you notice low levels on all outside calls, the PBX volume may be at fault. Compare volume of telephone utterances to badge user utterances. If telephone utterances are distinctly quieter, the PBX volume level may be too low.

Problems that appear in badge user utterances also appear in telephone system utterances. For example, you may hear clipped speech from an individual talking before the Genie is finished speaking.

Because individuals who call the hunt group or DID number are typically outside the Vocera system, the training that solves these problems may not be possible. If you can identify specific callers who regularly have these problems, suggest the solutions described in **Recording Badge User Utterances** on page 210.

Using Fixed-Length Numbers to Improve Recognition

Speech recognition problems can occur when people use the badge to send and respond to pages from inside and outside lines.

The Vocera administrator can specify Vocera Voice Server properties to limit phone extensions and pager numbers to a fixed length. Fixed-length numbers can improve speech recognition, because they eliminate from the grammar all possibilities that are not of the specified length. For details of these properties, see the *Vocera Telephony Configuration Guide.*

Speech Recognition Tips for Badge Users

Review a list of best practices for speech recognition in the Vocera environment.

Here are some things a badge user can do to improve speech recognition:

- Make sure the badge is close enough to your mouth.

  The microphone at the top of the badge must be directed toward your mouth, and it should be no closer than 6 inches and no farther than 8 inches (15 to 20 cm) away from your mouth.

- Wait for the Genie to finish speaking before giving a command or responding to a prompt.

  If you press the Call button and begin speaking immediately, your command may not be recognized. You must wait for the Genie to greet you before you give a command. (The Genie will say "Vocera" or will play a tone, or both, depending on your badge settings.)

  Sometimes, when the Genie gives a prompt that requires a "yes" or "no" answer (for example, "Should I save that message?"), the Genie will not "hear" you if you answer too quickly. Try waiting a moment before answering. You can also press the Call button to answer "yes," or press the Hold/DND button to answer "no."

- Speak a valid command in the proper format.

  The Genie recognizes specific commands, and these must be in the format verb-noun. Say the command first, and then give the details. Here are a few examples:

  "Call Jim Olsen."

  "Record a greeting."

  "Block all calls"

  "Play old messages."

- Train the Genie.

  If you think the Genie doesn't recognize a name or a command because of the way you pronounce it, you can train the Genie to understand you.

  To train the Genie, press the Call button, wait for the Genie to answer, and then say "Learn name" or "Learn command." You can also say "Learn group name" or "Learn location name" to train the Genie for other names.

  For detailed instructions, see "Training the Genie" in the *Vocera Badge User Guide*.

- Use the Speak or Spell feature.

  In addition to *speaking* the full name, you can *spell* the first name, the last name, or both names to contact users, groups, or address book entries. For example, you can use any of the following commands to place a call to the user or address book entry Jesse Hart:

  - Call Jesse Hart
  - Call J-E-S-S-E
  - Call H-A-R-T
  - Call J-E-S-S-E-H-A-R-T

Providing a Custom Help Prompt

In Vocera Voice Server 5.2.3 and later, the Help voice command allows you to interact with the Genie in natural language to receive information about voice commands and device features. Vocera recommends taking advantage of the built-in natural language capabilities of the system to provide user help. The rest of this section shows you how to override these built-in capabilities to provide a custom response to the Help command.

When you use this override capability, you record a custom Help prompt as a WAV file and place it in a specific folder on the Vocera Voice Server. The custom prompt then responds to the Help command, overriding it and providing users with specific site-based information (for example, the prompt could direct users to a Vocera super user, an administrator, an internal Web site, or a local help desk for assistance).

> **Note:** If you already have a custom help prompt and want to take advantage of the built-in natural language help capabilities, remove the custom prompt from the Vocera Voice Server and the system will begin using the natural language help capability.

To provide a custom Help prompt for your Vocera system:

1. Create a WAV file named `help_top_level.wav`.

   The WAV file must use the required audio format and sampling rate. See Required Format of Audio Prompt Files on page 214.

2. Place the `help_top_level.wav` file in the following folder on the active Vocera Voice Server:

   `\vocera\data\prompts\custom`

   > **Important:** Before putting a WAV file onto a production Vocera Voice Server, you should always test it first on a staging server. If the Nuance service is unable to play a WAV file because it was recorded incorrectly, the service throws an exception, which causes the Vocera Voice Server to restart.

3. If you have a Vocera Voice Server cluster, restart the standby nodes to force a remote restore. This causes the custom Help prompt to be replicated on the standby nodes.

4. To test the help prompt, log into a Vocera badge and say the command, "Help."
   The badge should play your custom WAV file.

   > **Note:** If the `help_top_level.wav` file is missing from the `\vocera\data\prompts\custom` folder, when a badge user says the "Help" command the system uses the standard Help prompt: "No help is currently available."

Required Format of Audio Prompt Files

Learn the needed formats for your audio promts.

If you create custom audio prompt files to use with Vocera, the WAV files must have the following format:

Audio Format: 16 bit Monophonic WAV PCM

Sampling Rate: 8000 samples/second

Important: Make sure audio prompt files used for alert tones are short in duration (no more than 2 seconds).

Appendixes

The appendixes provide reference information that help you administer Vocera. This includes:

- Best practices for device management processes for system device managers and group device managers.
- Best practices for entering values in all name fields in Vocera. Any name that you enter in Vocera has an effect on speech recognition.
- Rules for entering phone numbers, extensions, access codes, and macros in various phone number fields.
- A detailed description of the permissions that you can set when you create or modify a group.
- How to use Administration Console dialog boxes that prompt you for information.
- A discussion of the Emergency Broadcast feature which can be set at the group or site level.

Device Management Processes

This appendix provides a list of responsibilities, processes, and best practices for the system device managers and group device managers who use Vocera device management features.

Distribute this document to system device managers and group device managers to provide a quick summary of device management functionality in the Vocera Administration Console.

System Device Manager

This section describes system device manager reponsibilities and processes.

System Device Manager Responsibilities

Learn the duties of the System Device Manager in the Vocera System.

Key responsibilities for the system device manager include:

- Receiving devices into inventory when a new shipment arrives
- Configuring Vocera devices to connect to the wireless network
- Labeling devices
- Mapping device labels to serial number and MAC address
- Assigning devices to group or units
- Troubleshooting problems with devices
- Repairing devices and routing them back to the owning group
- Obtaining return merchandise authorization for nonfunctioning devices that are under warranty
- Retiring devices that are damaged and are no longer under warranty
- Tracking overall device utilization of the units and groups
- Ordering new Vocera devices

System Device Manager Processes

This section describes system device manager processes.

Beginning to Manage Devices

This topics describes the steps to follow in a scenario where a system device manager or group device manager needs to update information for a device.

To begin managing devices:

1. Open Internet Explorer and navigate to the Vocera Administration Console.
2. Log into the console.
3. Click Devices in the navigation bar.
4. Locate the record for a device using the Label, MAC Addr, or Serial No. field.
5. Select the record, and click Edit Device. The Add/Edit Device dialog box opens.

Note: The Add/Edit Device dialog box allows you to update only one device at a time. Alternatively, the Bulk Device Assignment dialog box can be used to assign status, owner, tracking date, and site values to multiple devices at a time. See **Bulk Device Assignment** on page 197.

Receiving New or RMA Replacement Devices into Inventory

This topics describes the steps to follow in a scenario where a system device manager receives devices that will be placed into inventory until they are needed by a department.

To receive new or RMA replacement devices into inventory:

1. Complete steps 1 to 3 in **Beginning to Manage Devices** on page 217.
2. Click Add New Device. The Add/Edit Device dialog box opens.
3. Update fields in the Add/Edit Device dialog box:
    a. Click the Select button to the right of the Owner field to select the group that maintains the inventory. At some facilities the Admin group may serve as the overall inventory owner. Generally, the owner of the device is a department group.
    b. In the Tracking Date field, you may want to enter the date the warranty for the device will expire. See **About Warranty and Tracking Dates** on page 218.
    c. Click the Select button to the right of the Site field to select the site where the device will be located. The site where the device is owned can differ from the site of the owning group.

       For instance, there could be a global group called Respiratory Therapists, however the device being assigned will be physically accounted for at a specific physical site, such as General Hospital. If your facility does not use sites, keep the default value of Global.
    d. In the Status field, select "Inventory" from the drop-down list.
    e. In the Notes field, enter the date, purchase order or invoice number, and your initials.
    f. Click Save, or continue scanning devices.

About Warranty and Tracking Dates

Vocera badges come with a limited warranty for one year from the shipment date to the original end user.

An additional one year warranty can be purchased at the time the badge is purchased. Vocera maintains the warranty date of record for all devices. The dates maintained by Vocera are the dates honored by the limited warranty contract. In no way will the data maintained in the Tracking Date field override the warranty data maintained by Vocera.

Labeling a Device

This topics describes the recommendations in a scenario where a system device manager needs to apply a physical label to a device to associate it with a group, unit, or user.

Recommendations: Use the following label maker and label:

- Any Brother P-touch® label maker that supports 3/8" tape and can connect to a computer. The connection to a computer is required to make it easier to create the labels since the data can come from a spreadsheet.
- Brother TZS221 Black on White Extra Strength P-touch Tape, 3/8" x 26.2'.
  Reference: **http://www.ptouchdirect.com/ptouch/tzs221.html**

For guidelines on the label text and where to apply the label to the device, see **Labeling Devices** on page 191.

Making a Device Active

This topics describes the steps to follow in a scenario where a system device manager receives a department request for one new device, or receives a device to replace one turned in for repair or RMA, or has repaired a device that now needs to be returned to a department.

To make a device active:

1. Remove a device from your stock.
2. Complete steps 1 to 5 in **Beginning to Manage Devices** on page 217.
3. Update fields in the Add/Edit Device dialog box:
   a. In the Label field, enter the label information from the physical label on the device. See **Labeling Devices** on page 191 for recommendations on how to label devices.

   > **Note:** Labels must be unique. If you want to use the same label as a device that has been retired, you must change the Label field for the retired device first. You can prepend the label of the retired device with the string "RETIRED-" or "RET-".

   b. Click the Select button to the right of the Owner field to select the group who will own the device. Generally, the owner of the device is a department group.
   c. Click the Select button to the right of the Site field to select the site where the device will be located.

   For instance, there could be a global group called Respiratory Therapists, however the device being assigned will be physically accounted for at a specific physical site, such as General Hospital. If your facility does not use sites, keep the default value of Global.

   d. In the Status field, select "Active" from the drop-down list.
   e. Check the Shared Device? box if the device will be shared among a group of users rather than assigned to a specific person.
   f. In the Notes field, enter today's date, notes indicating the device is being sent to the Group Device Manager and why, and your initials.
   g. Click Save.

Receiving a Device for Repair

This topics describes the steps to follow in a scenario where a system device manager receives a malfunctioning device to diagnose and evaluate for in-house repair or RMA submission.

To receive a device for repair:

1. Perform inspection and diagnostics on the malfunctioning equipment.
2. Complete steps 1 to 5 in **Beginning to Manage Devices** on page 217.
3. Update fields in the Add/Edit Device dialog box:
   a. In the Status field, select "Received for Repair" from the drop-down list.
   b. In the Notes field enter today's date, notes indicating the device was received and any conclusions reached resulting from the inspection and diagnostics, and your initials.
   c. Click Save.

Pending a Device for RMA

This topics describes the steps to follow in a scenario where a system device manager receives a malfunctioning device to diagnose and evaluate for in-house repair or RMA submission.

To make a device pending RMA:

1. Follow your existing process to request authorization to return the device to your support provider.
2. Complete steps 1 to 5 in **Beginning to Manage Devices** on page 217.
3. Update fields in the Add/Edit Device dialog box:
   a. In the Status field, select "Pending RMA" from the drop-down list.

b. In the Notes field, enter today's date, notes indicating an RMA is requested, and your initials.

c. Click Save.

RMA a Device

This topics describes the steps to follow in a scenario where a system device manager has received authorization to return a device for repair.

To RMA a device:

1. Complete steps 1 to 5 in Beginning to Manage Devices on page 217.
2. Update fields in the Add/Edit Device dialog box:
    a. In the Status field, select "RMA'ed" from the drop-down list.
    b. In the Notes field, enter today's date, notes indicating the RMA authorization number, the date when the device was mailed along with any tracking numbers, and your initials.
    c. Click Save.

Flagging a Device as Lost

This topics describes the steps to follow in a scenario where a system device manager has received a report that a device is lost or meets your facility's criteria to be categorized as lost.

To flag a device a device as lost:

1. Complete steps 1 to 5 in Beginning to Manage Devices on page 217.
2. Update fields in the Add/Edit Device dialog box:
    a. In the Status field, select "Lost" from the drop-down list.
    b. In the Notes field, enter today's date, any information regarding the lost device and how it qualified as lost, and your initials.
    c. Click Save.

Retiring a Device

This topics describes the steps to follow in a scenario where a system device manager has determined that the malfunctioning device is no longer under warranty or has non-warrantable damage. Avoid deleting devices; instead retire them. This will allow you to maintain historical data.

To retire a device:

1. Complete steps 1 to 5 in Beginning to Manage Devices on page 217.
2. Update fields in the Add/Edit Device dialog box:
    a. In the Status field, select "Retired" from the drop-down list.
    b. In the Notes field, enter today's date, notes indicating the reason for retiring the device, and your initials.
    c. Click Save.

Retiring a Device and Reusing the Label on a New Device

This topics describes the steps to follow in a scenario where the Label field for devices must be unique. Consequently, you cannot retire a badge and reuse the old label on a new device unless you change the old label first. The Label field is important for making Device Management reports clear and understandable.

To retire a device and reuse the label on a new device:

1. If you have not done so already, log into the Administration Console and create a Vocera group named "Retired Devices."
2. Complete steps 1 to 5 in Beginning to Manage Devices on page 217.
3. Update fields in the Add/Edit Device dialog box:

a. In the Label field, add "OLD-" to the beginning of the label and ".1" to the end of the label.

b. Click the Select button to the right of the Owner field. Select the "Retired Devices" group, and then click Finish.

c. In the Status field, select "Retired" from the drop-down list.

d. In the Notes field, enter today's date, notes indicating the reason for retiring the device, and your initials.

e. Click Save.

4. You can now assign the old badge label to a new badge. See **Labeling Devices** on page 191.

Group Device Manager

This section describes group device manager responsibilities and processes.

Group Device Manager Responsibilities

Learn the duties of a Group Device Manager in the Vocera environment.

Key responsibilities for the group device manager include:

- Analyzing reports of device inventory and recognition results by device
- Keeping track of the Vocera devices owned by the group and limiting the number of devices that get lost
- Ensuring that the Vocera devices are in good working condition
- Labeling devices (if not done by System Device Manager)
- Routing devices that need repair to the system device manager
- Maintaining a set of spare devices, batteries, and attachments
- Ensuring that users have the necessary Vocera accessories

Group Device Manager Processes

This section describes group device manager proceses.

Making a Device Active

This topics describes the steps to follow in a scenario where the Group Device Manager places a spare device into use in the department.

To make a device active:

1. Complete steps 1 to 5 in **Beginning to Manage Devices** on page 217.
2. Update fields in the Add/Edit Device dialog box:

   a. In the Status field, select "Active" from the drop-down list.

   b. In the Notes field, enter today's date, the reason for the change in status, and your initials.

   c. Click Save.

Returning a Device to the System Device Manager

This topics describes the steps to follow in a scenario where a group device manager has a malfunctioning device to return to the system device manager for diagnosis, repair, or replacement.

To return a malfunctioning device to the system device manager:

1. Perform any initial checks on the equipment to see if the device can be repaired on the unit.
2. Complete steps 1 to 5 in **Beginning to Manage Devices** on page 217.
3. Update fields in the Add/Edit Device dialog box:

   a. In the Status field, select "Sent for Repair" from the drop-down list.

b. In the Notes field, enter today's date, a description of the problem, and your initials.

c. Click Save.

d. Place the malfunctioning device into an RMA envelope and fill out the information per your facility's policy.

> **Note:** To order free RMA envelopes, visit Vocera's Print On Demand site: **http://www.vocera.com/printhq**

e. Follow your facility's policy for ensuring the device is delivered to the system device manager.

Making a Device Spare

This topics describes the steps to follow in a scenario where a group device manager places a device into the department's spares pool.

To make a device spare:

1. Complete steps 1 to 5 in Beginning to Manage Devices on page 217.
2. Update fields in the Add/Edit Device dialog box:
   a. In the Status field, select "Spare" status from the drop-down list.
   b. In the Notes field, enter today's date, note the change in status, and your initials.
   c. Click Save.

Flagging a Device as Lost

This topics describes the steps to follow in a scenario where a group device manager has received a report that a device is lost or meets your facility's criteria to be categorized as lost.

To flag a device as lost:

1. Complete steps 1 to 5 in Beginning to Manage Devices on page 217.
2. Update fields in the Add/Edit Device dialog box:
   a. In the Status field, select "Lost" from the drop-down list.
   b. In the Notes field, enter today's date, any information regarding the lost device and how it qualified as lost, and your initials.
   c. Click Save.

Monitoring the Status of Devices

This topics describes the steps to follow in a scenario where a group device manager wants to see who is currently using devices in a group.

> **Note:** You can monitor devices only for groups you are permitted to manage.

To see who is using devices in a group:

1. Open Internet Explorer and navigate to the Vocera Administration Console.
2. Log into the console.
3. Click Status Monitor in the navigation bar.
4. Click the Device Status tab.
5. Expand a group by clicking the triangle at the left of the group's name. The Device Status Monitor displays information for each active device.

Entering Spoken Names

As you create users, groups, and other entries in the Administration Console or the User Console, Vocera requires you to provide names.

These names are more than just a tag to let you visually identify an entry when you are using one of the consoles#mdash;they are words users can speak when placing calls, and they are words that the Genie speaks in interactions with badge users. Because all Vocera names have speech recognition consequences, the exact way you enter them in the console is very important.

The following table lists all the name fields in Vocera:

Table 81: Spoken name fields

Dialog Box	Name Fields
Add/Edit Site	• Site Name • Alternate Spoken Site Name
Add/Edit User	• First Name • Last Name • Alternate Spoken Names • Identifying Phrase
Add/Edit Group	• Group Name • Member Name - Singular • Member Name - Plural • Alternate Spoken Group Name
Add/Edit Location	• Location Name • Alternate Spoken Location Name
Add/Edit Address Book Entry	• First Name • Last Name • Name • Alternate Spoken Names • Identifying Phrase

The rest of this appendix shows you how to use these name fields to create spoken names that are intuitive and meaningful for users.

Rules for Entering Names

The value in any name field must start with a letter or digit.

It must contain only the following characters:

- Any of the 26 English letters, in lower or upper case
- Digits, such as 0, 1, 2, 3, and so forth
- Spaces
- Apostrophes (')
- Underscores (_)

- Dashes (-)

Names and Speech Recognition

The speech recognition system uses the values you enter in name fields to identify *entities* (users, groups, sites, locations, and address book entries).

Any name that a user speaks in a badge command must appear in one of the name fields so the speech recognition system can identify it.

Each of these entities has one or more primary name fields (for example, First Name and Last Name are the primary name fields for a user; Group Name is the primary name for a group) as well as one or more Alternate Spoken Name fields.

Use the primary name fields to enter the most common name of an entity. This name should be the one that most people use, *not* the "official" name. For example, if everyone calls the user "William Bones" by the name "Billy", you should enter "Billy" in the First Name field and "Bones" in the Last Name field.

If people often refer to users by something other than their primary names, such as a nickname or a title, you must also provide an alternate spoken name. For example, if people often call the user "Jason Crunch" by the nickname "Captain", you must enter "Captain Crunch" as his first alternate spoken name.

Similarly, if the user Rob Shostak is a doctor, enter his first and last names as usual, then enter "Doctor Shostak" as one alternate spoken name, and "Doctor Rob Shostak" as another alternate spoken name. This practice accommodates peers who call him "Rob Shostak", as well as nurses who typically call him "Doctor Shostak" or "Doctor Rob Shostak".

Because you cannot enter any letters except the 26 English letters in the Administration Console or User Console, you may sometimes have problems with user names. For example, you cannot enter common non-English characters such as ñ and é. If a user's name is "Louis Céline", you need to enter an approximation such as "Celine" in the console. In addition, if he uses the French pronunciation, or if other users refer to him with this pronunciation, you may need to add an alternate spoken name such as "Saline".

In general, however, do not provide alternate spoken names to accommodate a name that appears to have a "non-English" pronunciation, unless testing indicates that the system cannot recognize it. Vocera understands a wide variety of name pronunciations, and unnecessary alternate names increase the size of the database. An exception to this rule is slang or jargon that is often pronounced differently than it is spelled.

Using Numeric Values in Names

Because Vocera supports numeric and mixed alphanumeric values in name fields, you can create address book entries such as "911" or group names such as "Room 299".

Vocera supports the full range of common number pronunciations. For example, users can pronounce "Room 299" as either "Room Two Nine Nine", "Room Two Ninety Nine", or as "Room Two Hundred Ninety Nine" without creating alternate spoken names.

Previous versions of Vocera required you to spell any numbers that appeared in name fields. For example, you needed to enter names in the above example as "Nine One One" and "Room Two Nine Nine". These phonetic spellings limit users to a single pronunciation unless you provide alternate spoken names, which can be time consuming to enter and maintain. If you are using spelled numbers in a name field, consider converting them to numeric values for ease of maintenance and improved speech recognition.

Vocera supports the number pronunciations that are appropriate for different locales. For example, if you are using the UK locale, users can pronounce "7007" as "Seven Double Oh Seven", "Seven Double Naught Seven", "Seven Oh Oh Seven", and so forth.

Genie Number Pronunciations

Although Vocera allows *users* to say a full range of number pronunciations, the *Genie* always chooses a single pronunciation when responding to users.

If you don't like the Genie's pronunciation, you can record a name for the Genie to use when interacting with users in a voice command.

For example, suppose you have a group whose name is "Room 427". The Genie always pronounces this group as "Room Four Hundred and Twenty Seven", but users may pronounce it as "Room Four Twenty Seven". To change the Genie's pronunciation, use the "Record a Name" command to specify the name as "Room Four Twenty Seven".

Leading Zeros in Names

Because the Administration Console sorts names *alphabetically*, numeric values may sort differently than you expect.

For example, a group called I C U Nurse Bed 10 sorts before a group called I C U Nurse Bed 2.

To take advantage of numeric values and also have names sort as users expect, add leading zeros to the numbers so they have the same number of digits. For example, a group called I C U Nurse Bed 02 sorts before a group called I C U Nurse Bed 10.

Users do not have to pronounce these leading zeros to make a call; in fact, because leading zeros are ignored in common number pronunciations, users are not permitted to pronounce them. Consequently, a user sends a message to the I C U Nurse Bed 02 group by saying "Send a message to Eye See You Nurse Bed Two".

Using Ordinal Numbers in Names

An *ordinal* number specifies the position of an item in a sequence, such as "first", "second", or "third".

Although Vocera supports the full range of *number* pronunciations, it does not support common pronunciations of *alphanumeric ordinals* such as "1st", "2nd", or "3rd". For example, if you create groups whose names are "1st Floor" and "2nd Floor", Vocera expects you to pronounce them as "One-st Floor" and "Two-nd Floor".

Some organizations prefer to use alphanumeric ordinals in names because they sort in an expected order when you view them in the Administration Console. If you need to use alphanumeric ordinals, make sure you also create purely alphabetic alternate names to allow natural speech recognition. For example, if you are using "1st Floor" as a group name, create an alternate spoken name spelled as "First Floor" to support proper speech recognition.

Using Abbreviations in Names

Because the values you enter in name fields determine both what a user can say in a voice command and also how the Genie will pronounce names to a user, be careful when you enter abbreviations.

Follow these rules to ensure that you enter abbreviations correctly:

- If you want the Genie to pronounce the individual letters in an abbreviation, spell it in capital letters, with a space between the letters, and without periods. For example, enter the abbreviation for the American Federation of State, County and Municipal Employees as "A F S C M E".

  If you use one of the supported healthcare acronyms (see **Healthcare Acronyms and Abbreviations** on page 226), you can omit the spaces between the letters.

- If you want the Genie to pronounce an entry as a word, spell it as a word-that is, spell it with conventional capitalization and without unnecessary spaces between the letters. For example, enter the name Bob Ray as "Bob Ray", not as "BOB RAY".

If you follow these rules, the Genie will always say what you intended. If you *do not* follow these rules, you may unintentionally create problems. The third-party software Vocera uses to provide text-to-speech translation may incorrectly interpret a string of capital letters as either an abbreviation or a word, depending on the number of letters in the string.

Using Slang and Jargon in Names

Users often speak slang or jargon for group names and address book entries, and you should accommodate these existing speech patterns, rather than requiring users to learn other names.

Because slang and jargon often originate as either acronyms or the clipped form of words, they are often pronounced very differently than they are spelled, and you typically need to enter alternate spoken names to support them.

An *acronym* is an abbreviation that is pronounced as a word. For example, in a hospital, the Medical Intensive Care Unit is often abbreviated as "MICU" and pronounced as "Mick You". To accommodate this usage, Vocera supports several healthcare acronyms as part of the static grammar. See Healthcare Acronyms and Abbreviations on page 226.

Similarly, longer words such as "Pediatrics" are often spelled with the clipped form "Peds", but pronounced as "Peeds" (not "Peds", as the spelling implies). To accommodate this usage, enter "Pediatrics" in the Group Name field, and enter "Peeds" in the Alternate Spoken Group Name field.

The best practice in this situation is to enter the name as users spell it in the Group Name field and to enter phonetic variations in the Alternate Spoken Group Name field. This practice allows the expected and more readable name to appear in the user interface of the consoles, but still supports the spoken name preferred by users.

Healthcare Acronyms and Abbreviations

The Vocera system supports the following standard acronyms and abbreviations for the healthcare industry as part of the static grammar.

You can embed these healthcare acronyms within group names. Spaces in an acronym are optional and can be omitted. For example, you can enter "MICU Charge Nurse" instead of "M I C U Charge Nurse". When one of these acronyms is used in a group name, users can pronounce either the letters in the acronym (for example, "M I C U") or the acronym itself (for example, "Mick You") to call the group.

Note: These acronyms and abbreviations should NOT be entered in the Alternate Spoken Group Name field. Otherwise, the alternate spoken group names could interfere with the recognition of the acronyms and abbreviations. Also, if you use acronyms or abbreviations in a group name, you should record the proper pronunciation of the group name. The Genie will then use your recorded prompt(s) for more natural sounding speech.

Table 82: Healthcare acronyms and abbreviations

Acronym/Abbreviation	Pronunciation
C C U	"C C U"
C M O	"C M O"
C N O	"C N O"
E D	"E D"
E K G	"E K G"

Acronym/Abbreviation	Pronunciation
E N T	"E N T"
E R I	"E R I"
I C U	"I C U"
I V	"I V"
L and D	"El and D"
L V N	"L V N"
M I C U	"Mick You" or "M I C U"
M R I	"M R I"
M U C	"M U C"
N I C U	"Nick You" or "N I C U"
O B G Y N	"O B G Y N"
O R	"O R"
P A C U	"Pack You" or "P A C U"
P I C U	"Pick You" or "P I C U"
P T	"P T"
Pre Op	"Pre Op"
R A D O N C	"Rad Onk" or "R A D O N C"
Rad Onc	"Rad Onk"
R T	"R T"
S I C U	"Sick You" or "S I C U"

You can use Vocera Professional Services to customize the list of group name acronyms for your Vocera system. For more information, contact Vocera Professional Services.

Entering Phone Numbers

Vocera allows you to enter various types of phone numbers.

For example, when you add a user to the Vocera system, you can specify the user's desk extension, cell phone number, pager number, and home phone number. Similarly, groups and address book entries also have phone numbers associated with them.

In Vocera, the value of a phone number can contain any of the following characters:

- Digits. Any of the following characters: 0123456789.
- Special dialing characters.
- Special dialing macros.
- PIN template macros.

Vocera ignores any other character that you enter in phone number fields. For example, you can enter **(408) 790-4100**, to make a number more readable, instead of **4087904100**. Vocera ignores the extra spaces, dashes, and parentheses when the number is actually dialed. However, Vocera may add access codes or area codes to numbers before dialing.

> **Note:** Entering a number in a console field does not guarantee that a user will be able to call that number.

About Call Types

You can specify whether a group has permission to make various types of calls, and users acquire calling permissions through group membership.

To grant or revoke permissions for specific call types in the Administration Console, use the **Groups** screen > **Add/Edit** page > **Permissions** tab.

Vocera recognizes the following call types:

Table 83: Call types

Call Type	Description
Internal	A number on your side of the PBX. For example, a call to a desk extension or internal pager is an internal call. Vocera dials these numbers without adding any other codes. The Call Internal Numbers permission controls a group's ability to make internal calls.

Call Type	Description
Outside	A number on the other side of the PBX. For example, a call to a business or residence or service or outside pager is an outside call. There are two types of outside call, toll-free and toll: • By default, a call within the specified local area code is **toll-free**. Therefore, you must grant a group Call Toll-Free Numbers permission to enable members of that group to make local calls. Vocera omits or includes the area code when making a local call, depending on the value of the **Omit Area Code when Dialing Locally** field. Vocera also adds any access codes you need to get an outside line, such as a **9**. • By default, any other call is considered a **toll call**. For example, domestic or international long distance calls are toll calls. The Call Toll Numbers permission controls a group's ability to make toll calls. For domestic long distance calls, Vocera adds any access codes you need to get an outside line, such as a **9**, and any numbers you need to specify a long distance call, such as a **1** or a **0**. The format for an international long distance number depends on the locale of the Vocera Voice Server. Typically, you specify the complete dialing sequence, including access codes and country codes, as appropriate, and Vocera dials the string as-is.

You can override Vocera's default handling of internal and outside calls (for example, you can define an outside area code to be toll-free). Use the Telephony section of the Administration Console to customize this behavior.

Phone Number Rules

The following rules define how Vocera interprets a value in a phone number, pager number, or extension field in the Administration Console or the User Console.

These requirements include:

- A value that starts with the letter X (for example, X1234) represents an **internal number** (for example, a desk extension or an inside pager number).
- A value that starts with the letter Q (for example, Q901114087904100) represents a number to be interpreted **literally**. Vocera dials such numbers as-is, without adding any access codes or area codes.
- Vocera also interprets a value with 6 or fewer digits as an **internal number**. However, for clarity, it's best to type the letter X before such values to make the meaning explicit. On a Vocera system configured for the UK locale, you must type the letter Q before an outside number of 6 or fewer digits (for example, Q9100 specifies an access code and a short code service number) to make Vocera dial the number as-is.
- A value longer than the maximum length for the locale is also interpreted **literally**. The following table lists the maximum phone number length, including area code, for each supported locale.

Table 84: Maximum phone number length per locale

AU	CA	GB	NZ	US
10 digits	10 digits	11 digits	11 digits	10 digits

- Some locales define a fixed length for telephone numbers. When a phone number field value is of this length, it represents a **local outside number**. For example, a Vocera system configured for the US locale interprets a 7-digit value as an outside number within the local area code. The following table lists the fixed length of local numbers, *not* including area code, defined for each supported locale.

Table 85: Fixed length of local numbers per locale

AU	CA	GB	NZ	US
Not defined	7 digits	Not defined	7 digits	7 digits

- In any other case, the value represents an outside number. Vocera adds access codes and applies **long distance** and **toll call** rules as appropriate. For clarity, it's best to include the area code with any outside number, local as well as long distance.

Vocera uses the same rules to interpret phone numbers spoken through voice commands, with the following additional limitations:

- You cannot use special dialing characters in a voice command.
- You cannot specify an extension of seven or more digits in a voice command.
- You must include the area code when speaking an outside number.

Special Dialing Characters

A *special dialing character* is a non-numeric character that you can enter in a field in the Administration Console or the User Console that requires an access code, phone number, or extension.

For example, you can use an asterisk (*) to simulate pressing the star key on a touch-tone phone, or enter an X at the beginning of a number to tell Vocera to treat that number as an extension.

Vocera supports the following special dialing characters:

Table 86: Special dialing characters

Character	Effect
,	When connecting to an analog PBX, pauses for two seconds before dialing the next digit. Use a comma to force Vocera to pause briefly during a dialing sequence. Use multiple commas if you need to pause for more than two seconds. For example, suppose your system requires you to dial **9** as the local access code, but it is slow to establish an outside line. If you enter **9,** in the Default Local Access Code field, Vocera dials a 9 and then pauses to let the system establish the outside line before continuing with anything following in the dialing sequence. Do not use a comma when you are connecting to a digital PBX. The comma character is not recognized by a digital PBX, and it may prevent a connection. However, you can use commas in sequences issued after a connection is made. For example, you can use commas to the right of a semicolon.
;	Separates the data Vocera uses to connect a call from any data Vocera passes through after the call is established. Characters to the left of the semicolon are used to establish the connection, and characters to the right of the semicolon are passed through after the connection is made. For example, you may need to use a sequence of characters such as the following to forward calls to a pager: `Q 9, 1 (408) 555-1313 ; %V %D #` In this sequence, `Q 9, 1 (408) 555-1313` establishes the connection; the *Q* tells Vocera not to prepend an access code or area code, the *9* gets an outside line, and the remaining characters indicate the phone number to call. The *%V %D #* characters are pass-through values (the *%V* and *%D* are dialing macros, and the # is required by the pager to end the sequence). Important: For any dialing string that includes a semicolon (;), the Vocera Telephony Gateway server automatically appends a # to end the sequence.
&	Simulates pressing the flash key on a touch-tone telephone.
#	Simulates pressing the pound key (also called the hash key) on a touch-tone telephone.
*	Simulates pressing the star key on a touch-tone telephone.

Character	Effect
X	Tells Vocera to treat the sequence of digits following this special dialing character as an extension, without prepending either an access code or an area code to them. Vocera ignores this character unless it is the first character of the number. This special dialing character is not case-sensitive.
Q	Tells Vocera to dial the sequence of digits following this special dialing character as a literal value, without prepending either an access code or an area code to them. Vocera ignores this character unless it is the first character of the number. This special dialing character is not case-sensitive.

Special Dialing Macros

A *dialing macro* represents a dialing sequence.

In data entry fields where you cannot enter a specific number—because the number varies with the user who accesses the feature—you can enter a dialing macro. Vocera replaces the macro with the actual number on demand.

Dialing macros are especially useful when editing Company Voicemail Access Codes and Address book entries. For example, the Company Voicemail Access Code field specifies the dialing sequence that Vocera uses to forward an incoming call to company voicemail. As part of the dialing sequence, you typically need to specify a desk phone extension to identify the voice mailbox you want to access. You cannot enter a specific desk extension in this field, because the number will vary depending on which user is forwarding calls. Instead, you use the **%D** macro as part of the dialing sequence. Vocera replaces that macro with the actual desk extension of the user who is forwarding calls.

Vocera supports the following dialing macros, listed in alphabetical order:

Table 87: Dialing macros

Macro	Effect
%C	Inserts the user's cell phone number into a data entry field. This macro expands to the value of the **Cell Phone** field of the Phone page in the Add/Edit User dialog box. A user can also enter or change this value in the User Console.
%D	Inserts the user's extension (either the Desk Phone or Extension, Vocera Extension, or dynamic extension, whichever applies) into a data entry field. You can enter or change the value of the **Desk Phone or Extension** field or the Vocera Extension field on the Phone page in the Add/Edit User dialog box. A user can also enter or change these values in the User Console.
%H	Inserts the user's home phone number into a data entry field. This macro expands to the value of the **Home Phone** field of the Phone page in the Add/Edit User dialog box. A user can also enter or change this value in the User Console.
%V	Inserts the Vocera hunt group or DID number into a data entry field. This macro expands to the value in the **Vocera Hunt Group Number** field on the Basic Info page of the Telephony screen.

PIN Template Macros

Each PBX has different rules for adding a PIN to a dialing sequence.

Some require the phone number followed by the PIN. Some require the PIN before the phone number. Some require an access code for an outside line, or a feature code to indicate that a number is a PIN. Some require a separator character between the PIN and the number. A telephony PIN template can use macros to specify and format the information in a PIN.

Vocera provides the following macros for specifying a PIN template:

Table 88: PIN template macros

Macro	Effect
%A	Expands to the value of the access code for the phone number being dialed.
%M	Expands to the value of the phone number being dialed.
%N	Expands to the value of the access code for the phone number being dialed, followed by the phone number. The %N macro is the equivalent of the %A macro followed by the %M macro.
%P	Expands to the value in one of the following fields, listed in descending order of precedence: • The **PIN for Long Distance Calls** field in the Phone page of the Add/Edit User dialog box. • The **PIN for Long Distance Calls** field in the Department page of the Add/Edit Group dialog box. • The **PIN for Long Distance Calls** field in the PIN page of the Telephony section.

The %A and %M macros are useful for inserting a PIN into the dialing sequence (for example, between the access code and the number) instead of appending it.

Example PIN Templates

The following table lists some example PIN templates, along with descriptions and the values sent by the Vocera system to the PBX.

The results are based on the following assumptions:

- The user belongs to a group that allows toll calls.
- The user's PIN is **1234**.
- The phone number **(213) 555-0945** is a long distance call.
- The long distance access code (if required) is **91**.
- The feature code for a PIN (if required) is ***88**.

Table 89: PIN template examples

PIN template	Result	Description
%N %P	912135550945 1234	Access code, phone number, PIN.
%M %P	2135550945 1234	Phone number, PIN.
%A, %M %P	91, 2135550945,1234	Access code, pause, phone number, PIN.
%P, %A %M	1234, 91 2135550945	PIN, pause, access code, phone number.
%A *88 %P %M	91 *88 1234 2135550945	Access code, feature code, PIN, phone number

How Vocera Builds a Dialing Sequence

When a user issues a voice command to dial a telephone number or forward a badge call to a telephone or to voice mail, Vocera sends the phone system a sequence of digits to dial.

In addition to the phone number itself, the sequence may contain the access codes needed to obtain an outside line (such as a **9**), to dial long distance (such as a **9** followed by a **1**), or to access company voicemail.

You do not enter these access codes as part of a phone number. You set up these access codes for your entire organization, and Vocera adds them to phone numbers as necessary before dialing. For example, the following figure shows the flow of events that occur when a badge user places a long distance call to a person who is listed in an address book entry.
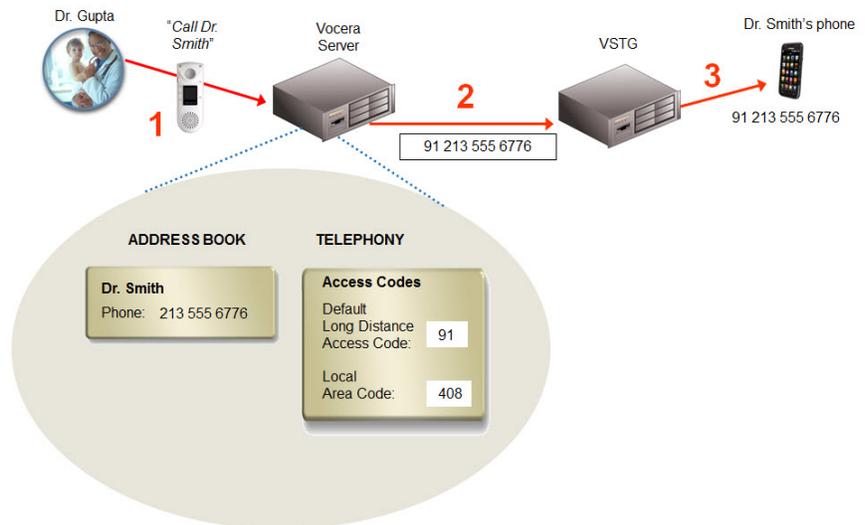
Figure 27: Placing a long distance call

In this situation, the following events occur:

1. Dr. Gupta tells the Genie to call Dr. Smith.

   The Vocera Voice Server finds Dr. Smith's telephone number in the address book, then adds long distance access codes to the dial string because Dr. Smith's area code is different from the local area code.

2. The Vocera Voice Server tells the Telephony server to dial the number.

3. The Telephony server dials the number.

Permissions Reference

This section provides a detailed description of the permissions that you can set when you create or modify a group.

The permissions are listed in the order in which they appear in the Administration Console, and they are sorted into categories based on their function. Icons help you identify the category in which each permission belongs.

System Administrator Permissions

The table in this topic summarizes the system administrator permissions.

Table 90: System administrator permissions

System Admin Permission	Description
Perform System Administration	Gives a group full administrative privileges in the Administration Console, and automatically grants those group members every permission except for the ones that administrators do not need: • Require Authentication to Log In • Require Authentication to Play Messages This permission overrides any revoked permissions inherited by membership in other groups, except the revoked Perform Server Administration permission itself.
Record Name Prompts for Another User	Grants permission to record name prompts for other users, as well as groups and address book entries. Name prompts improve the usability of the Vocera system; the Genie plays these name prompts when necessary, instead of synthesizing speech.

Tiered Administrator Permissions

The table in this topic summarizes the tiered administrator permissions.

Table 91: Tiered administrator permissions

Tiered Admin Permission	Description
Add/Edit/Delete Users	Grants a tiered administrator permission to maintain the Vocera database by adding, editing, and deleting users and all features in their profiles, such as alternate spoken names, group membership, and so forth.
Edit Users	Grants a tiered administrator permission to maintain the Vocera database by editing existing user profiles.
Add/Edit/Delete Temporary Users	Grants a tiered administrator permission to maintain the Vocera database by adding, editing, and deleting temporary users and all features of their profiles.
Add/Edit/Delete Address Book Entries	Grants a tiered administrator permission to maintain the Vocera database by adding, editing, and deleting address book entries. Also grants permission to record a spoken name for address book entries.

Tiered Admin Permission	Description
View Users and Groups	Grants a tiered administrator permission to monitor user and group activity, view their profiles, and generate lists of them in reports. Also allows viewing information about address book entries.
Perform System Device Management	Grants a tiered administrator permission to add, edit, and delete device data, including device status values, for all sites, and to view the Status Monitor.

Call Permissions

The following table summarizes the call permissions. Several of these permissions require Telephony Integration. See the *Vocera Voice Server Telephony Configuration Guide* for more details.

Table 92: Call permissions

Call Permission	Description
Call Internal Numbers	Grants permission to place calls to internal telephone extensions by saying the key phrase "Dial extension" (for example, "Dial extension 4085"). This feature requires Telephony Integration.
Call Toll-Free Numbers	Grants permission to place calls to phone numbers in toll-free calling areas. This feature requires Telephony Integration.
Call Toll Numbers	Grants permission to place calls to phone numbers that are not in toll-free calling areas. This feature requires Telephony Integration.
Forward Calls to Badges	Grants permission to forward incoming calls to other badges. When this permission is granted, users can specify forwarding options through either the User Console or voice commands.
Forward Calls to Internal Numbers	Grants permission to forward incoming calls to internal phone numbers. This feature requires Telephony Integration. When this permission is granted, users can specify forwarding options through either the User Console or voice commands.
Forward Calls to Toll-Free Numbers	Grants permission to forward incoming calls to phone numbers in toll-free calling areas. This feature requires Telephony Integration. When this permission is granted, users can specify forwarding options through either the User Console or voice commands.
Forward Calls to Toll Numbers	Grants permission to forward incoming calls to phone numbers that are not in toll-free calling areas. This feature requires Telephony Integration. When this permission is granted, users can specify forwarding options through either the User Console or voice commands.
Initiate Broadcasts	Grants permission to broadcast to all users in any group except Everyone or Everyone Everywhere.
Initiate Broadcasts to Everyone	Grants permission to broadcast to all users in your site's Everyone group or the Everyone Everywhere group.
Initiate Urgent Broadcasts	Grants permission to broadcast an urgent call to every member in a group at the same time. An urgent broadcast has priority and breaks through to everyone's badge, even if the badge is blocking calls or is in DND mode. See the *Vocera Badge User Guide* for more information about urgent broadcasts.
Place Urgent Calls	Grants permission to place an urgent call or initiate an urgent three-way conference call. An urgent call or urgent three-way conference call has priority and breaks through to a badge, even if the badge is blocking calls or is in DND mode. See the *Vocera Badge User Guide* for more information about urgent calls.
Call Users at Other Sites	Grants permission to contact a user whose home site or current site is different than the home site or current site of the caller.

Call Permission	Description
Join Conference	Grants permission to enter or leave a conference. Vocera does not require users to have a permission to use a conference; that is, any user who is in a conference has access to the conference feature. To prevent a user from conferencing, deny the conference permission and use the Administration Console to remove the user from a conference.
Send Messages to Everyone	Grants permission to send a message to all users in your site's Everyone group or the Everyone Everywhere group.
Have Toll-Free Pager Number	Grants permission to have a pager number that is in a toll-free calling area. This feature requires Telephony Integration. Vocera does not require users to have permission to call pagers. If you allow users the permission to *have* pager numbers, you are implicitly allowing other users the permission to *call* those numbers, regardless of their calling permissions.
Have Toll Pager Number	Grants permission to have a pager number that is in a toll calling area.This feature requires Telephony Integration. Vocera does not require users to have permission to call pagers. If you allow users the permission to *have* pager numbers, you are implicitly allowing other users the permission to *call* those numbers, regardless of their calling permissions.

Special Permissions

The table in this section summarizes the special permissions.

Table 93: Special permissions

Special Permission	Description
Locate Users or Group Members	Grants permission to issue commands such as "Where is Melissa Schaefer?" to find the physical location of a user or group member. This feature is useful only if location names have been defined and access points have been assigned to locations. See Working with Locations on page 41.
Have VIP Status	Grants permission to complete a call even when users are blocking calls or have placed their badges in Do Not Disturb mode. The Genie tells a VIP caller that a person is not accepting calls and asks if the caller wants to break through. If the answer is "Yes," the call is connected. If the answer is "No," the call is treated as an unanswered call.
Block and Accept Calls	Grants permission to issue the Block and Accept voice commands to perform selective call screening. Beginning users who are granted this permission may unintentionally block calls when all they need is temporary use of the DND button. You should enable these commands for advanced users only. This permission does not affect the ability to block calls through the User Console.
Access Vocera Anywhere Using Caller ID	Grants permission to call the Vocera hunt number from a phone and access the Genie using a caller ID associated with the phone. The caller's ID is matched against a user's desk phone number or cell phone number in the Vocera database.

Pop-Up Dialog Box Reference

The Administration Console displays dialog boxes that prompt you for information.

This section explains how to use these pop-up dialog boxes.

Select Group

The Select Group dialog box lets you choose from a list of groups that are already defined in the Vocera system.

To display this dialog box, click the Select button next to any field that requires you to enter a group name.

Follow these steps to use the Select Group dialog box:

1. Choose a group name from the list.
2. Click Finish.

   The Select Group dialog box closes, and the name appears in the field next to the Select button.

To search for a name in the list:

1. Begin typing the name in the Search field. As you type, the Vocera Voice Server finds the closest match.
2. Click Finish.

   The Select Group dialog box closes, and the name appears in the field next to the Select button.

Select User or Group

Use the Select User or Group dialog box to choose from a list of users and groups defined in the Vocera system.

To display this dialog box, click the Select button next to any field that requires you to enter the names of users or groups.

This dialog box displays icons to help you identify the names:

- Users have badge icons next to their names.
- Groups have face icons next to their names.

To select a user, group, or address book entry:

1. Click a name.
2. Click Finish to close the dialog box.

   The name appears in the field next to the Select button.

To select multiple names:

1. Hold down the Ctrl key as you click each name.

2. Click Finish to close the dialog box.

   The names appear in the field next to the Select button.

To select a range of names:

1. Click the first name in the range.
2. Hold down the Shift key as you click the last name in the range.
3. Click Finish to close the dialog box.

   The names appear in the field next to the Select button.

To search for a name in the list:

1. Begin typing the name in the Search field.
   - Type the name of a group, the name or a place that is an address book entry, the last name of a user, or the last name of a person who is an address book entry.
   - If the list contains many users with the same last name, type a comma and space after the last name and continue with the first name.

     As you type, the Vocera Voice Server finds the closest match.
2. Click Finish to close the dialog box.

   The name appears in the field next to the Select button.

Select User, Group, or Address Book Entry

The Select User, Group, or Address Book Entry dialog box lets you choose from a list of users, groups, and address book entries that are already defined in the Vocera system.

You can display this dialog box by clicking the Select button next to any field that requires you to enter the names of one or more users, groups, or address book entries.

This dialog box displays icons to help you identify the names:

- Users have badge icons next to their names.
- Groups have face icons next to their names.
- Address book entries have face icons with address books next to their names.

To select a user, group, or address book entry:

1. Click a name.
2. Click Finish to close the dialog box.

   The name appears in the field next to the Select button.

To select multiple names:

1. Hold down the Ctrl key as you click each name.
2. Click Finish to close the dialog box.

   The names appear in the field next to the Select button.

To select a range of names:

1. Click the first name in the range.
2. Hold down the Shift key as you click the last name in the range.
3. Click Finish to close the dialog box.

   The names appear in the field next to the Select button.

To search for a name in the list:

1. Begin typing the name in the Search field.

- Type the name of a group, the name or a place that is an address book entry, the last name of a user, or the last name of a person who is an address book entry.
  - If the list contains many users with the same last name, type a comma and space after the last name and continue with the first name.

    As you type, the Vocera Voice Server finds the closest match.

2. Click Finish to close the dialog box.

   The name appears in the field next to the Select button.

Select Site

The Select Site dialog box lets you choose from a list of sites that are already defined in the Vocera system.

You can display this dialog box by clicking the Select button next to any field that requires you to enter a site name.

Note: This function can only be performed by a site administrator for a user.

To use the Select Site dialog box:

1. Choose a site name from the list.
2. Click Finish.

   The dialog box closes, and the name appears in the field next to the Select button.

To search for a name in the list:

1. Begin typing the name in the Search for Site field.

   As you type, the Vocera Voice Server finds the closest match.
2. Click Finish.

   The Select Site dialog box closes, and the name appears in the field next to the Select button.

Select Location

The Select Location dialog box lets you choose a neighboring location from a list of locations that are already defined in the Vocera system.

You can display this dialog box by clicking the Add button on the Neighbors page of the Add New Location or Edit Location dialog box.

To select a neighbor:

1. Click a name.
2. Click Finish. The dialog box closes, and the name appears in the Neighbor Location field on the Neighbors page.

To select multiple neighbors:

1. Hold down the Ctrl key as you click each location.
2. Click Finish. The dialog box closes, and the names appear in the Neighbor Location field on the Neighbors page.

To select a range of neighbors:

1. Click the first name in the range.
2. Hold down the Shift key as you click the last name in the range.
3. Click Finish. The dialog box closes, and the names appear in the Neighbor Location field on the Neighbors page.

To search for a location in the list:

1. Begin typing the name in the Search field. As you type, the Vocera Voice Server finds the closest match.

2. Click Finish. The dialog box closes, and the name appears in the Neighbor Location field on the Neighbors page.

Choose Subdepartments

The Choose Subdepartments dialog box lets you choose which subgroups contained within a department are designated as subdepartments.

You can display this dialog box by clicking the Choose Subdepartments button on the Departments page of the Administration Console, or by double-clicking a department or subdepartment that has subgroups.

> **Note:** You can also designate a group as a Department or Subdepartment by editing the group and changing the value of the **Group Type** field on the Departments tab of the Add/Edit Group dialog box.

To choose subdepartments:

1. In the Subgroups list, select any groups that you want to make subdepartments, and then click >> to move them into the Subdepartments list.

2. In the Subdepartments list, select any groups that you want to make subdepartments, and then click << to move them into the Subdepartments list.

3. Click Save to save the settings and close the Choose Subdepartments dialog box.

Emergency Broadcast Groups

Vocera provides a scalable emergency notification feature that is set at the site or group level in the Administration Console.

Emergency broadcasts are initiated on the badge when you click the Call button on your Vocera badge twice. You can also initiate an emergency broadcast from the Vocera Collaboration Suite on your cell phone. When an emergency broadcast is triggered, everyone in the group hears the caller immediately—no speech recognition or Genie interactions are necessary.

Support for Multiple Emergency Groups

If your organization requires more than one *emergency broadcast group* or needs the emergency group set to a specific functional group, you can do so at the group level. This feature provides the flexibility to meet the emergency needs of different departments, each with their own set of responders.

Site and Group Level

At the site level you can designate an existing group as the emergency broadcast target group, or add specific members to a group utilizing it as the emergency broadcast target. However, each site can have only **one** emergency broadcast target group.

Similarly, at the group level you can designate an existing group as the emergency target, or add specific members to a group which can be used as the emergency responders. However, at the group level, you can have multiple emergency broadcast target groups, each one designated to a different emergency broadcast initiating group.

Default Behavior

If a user is not a member of a group that has a designated emergency broadcast target group, an emergency broadcast is delivered to the site level emergency target group (if configured) when an urgent broadcast is initiated. In addition, If a emergency broadcast group is not designated at the site or group level, the default behavior is to use the emergency broadcast target group set at the Global site.

If the emergency broadcast initiator triggers a site-level emergency, it will preempt or cut through any members already receiving a group emergency broadcast.

The Everyone and Everyone Everywhere group cannot be designated as an emergency broadcast group. In the Administration Console, the Emergency Broadcast field is not available on the Edit Group dialog box for either of these groups.

Assigning Emergency Broadcast Groups

From the Groups or Sites screen:

1. On the Group or Sites tab, click Add New Group/Site or Edit Group/Site. The Add/Edit New Group/Site dialog box opens.

Figure 28: Add New Group dialog box

2. From the Add/Edit New Group/Site dialog box on the Info tab, click the Select button. The Select Group dialog box opens and displays the list of available groups.
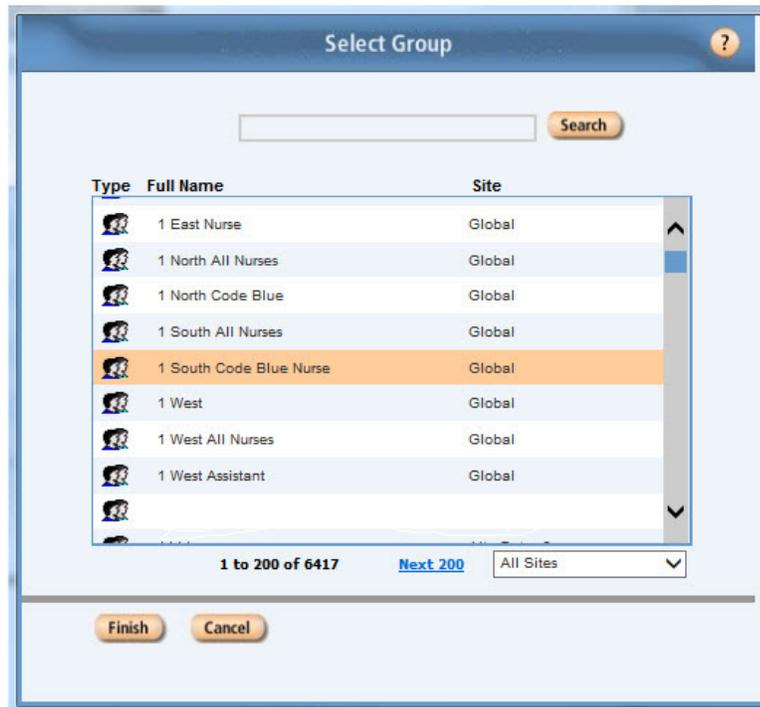
Figure 29: Select Group dialog box

3. From the group list, highlight the group that you want to designate and click Finish. The Select Group dialog box closes and the chosen group is displayed in the Emergency Broadcast Group field on the Add New Group or Edit New Group dialog box.

4. Click Save.

Setting Up Silent Emergency Broadcasts

After you set up the emergency broadcast group for your site, you can specify whether to initiate emergency broadcasts silently, without playing a chime.

1. On the Sites tab, click Add New Site or Edit New Site. The Add / Edit New Site dialog box opens and lists the selected group in the Emergency Broadcast Group field.

2. From the Add New Group/Site dialog box, select the check box next to Initiate Emergency Broadcast Silently.
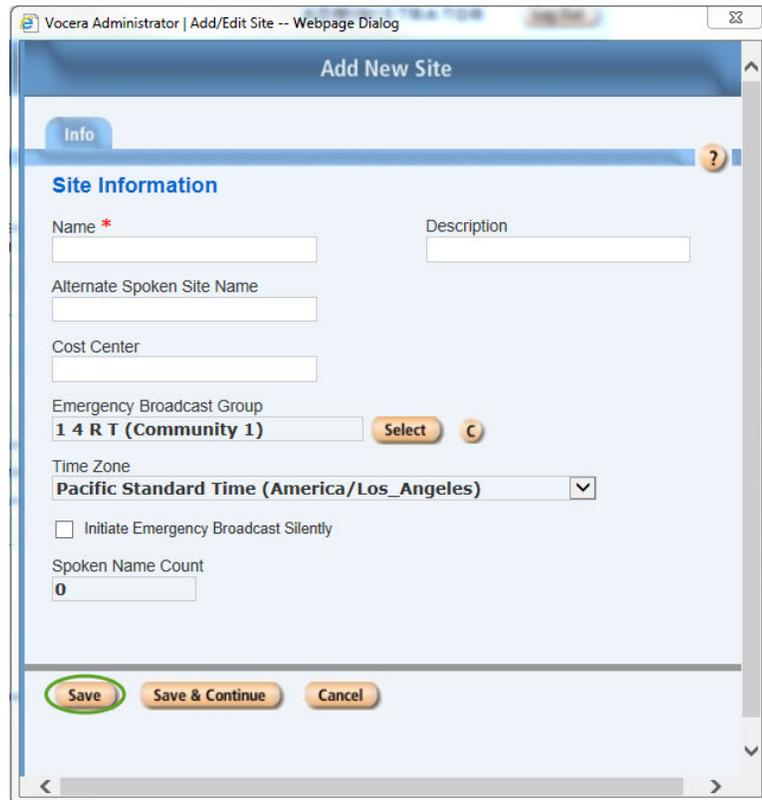
Figure 30: Add New Site dialog box

3. Click Save.