stryker

Vocera Platform Administration Guide

Version 6.1.0

Notice

Stryker Corporation or its divisions or other corporate affiliated entities own, use or have applied for the following trademarks or service marks: Stryker, Vocera. All other trademarks are trademarks of their respective owners or holders. The absence of a product or service name or logo from this list does not constitute a waiver of Stryker's trademark or other intellectual property rights concerning that name or logo. Copyright © 2023 Stryker.

Last modified: 2023-02-14 08:23

Acapella-610-Docs build 1190

Contents

Getting Started 12

About the Vocera Platform 13

About the Vocera Platform Administration Guide 14

Related Documentation 15

Using the Vocera Platform Web Console 16

About Vocera Platform Web Console 16

Browser Requirements 17

Logging Into the Vocera Platform Web Console 17

Logging Out 18

Setting Presence and Availability 19

Messaging 21

About the Vocera Vina Web User Guide 22

About Conversations 23

Starting a Conversation 23

Starting a Group Chat 25

Adding a Message 28

Message States 30

Sending a Quick Response 30

Acknowledging a Message 31

Conversations with Unread Messages 32

Viewing Participants 33

Adding a Participant to a Conversation 34

Leaving a Conversation 36

Searching Conversations 36

About Templates 38

Using a Staff Template 38

Using a Patient Template 39

Completing a Template Message 41

About Personal Messages 43

About Mass Notifications 44

About Favorites 45

Adding a Favorite 45

Personal Titles 48

Staff Assignment ... 49
About the Vocera Platform Staff Assignment Guide ... 50
Staff Assignment Prerequisites ... 50
Configuring Staff Assignment ... 51
Creating a Staff Assignment Facility ... 51
Importing Beds, Rooms, and Departments ... 52
Enabling Matching Rules for Import ... 54
Creating Locations ... 54
Creating Functional Roles ... 57
Assigning Roles and Linking Groups ... 58
Assigning Department Level Permissions ... 60
The Staff Assignment Home Page Layout ... 62
Using Staff Assignment ... 64
Viewing Departments ... 64
Setting a Department to Home Department ... 65
Viewing and Searching Staff Members ... 66
Assigning Staff Member by Clicking ... 67
Assigning Staff Member by Replacing ... 68
Assigning Staff Member by Typing ... 70
Assigning Staff Member using Copy and Paste ... 71
Messaging Care Team ... 73
Messaging an individual Staff Member ... 75
Removing a Staff Assignment ... 76
Adding Notes for a Patient ... 77
My Profile ... 79
About the Vocera Platform My Profile Guide ... 80
The My Profile Home Page Layout ... 81
Working With My Profile ... 83
Viewing and Editing General Profile Information ... 83
Viewing and Editing Login Information ... 84
Adding Contact Information ... 85
Viewing Group Membership ... 85
Adding Groups ... 86
Removing Groups ... 86
Viewing and Configuring Voice Service Fields ... 87
Configuring Speech Recognition ... 88
Configuring Call Forwarding ... 90
Configuring Call Blocking ... 91
Configure Genie Settings ... 92
Notifications and Miscellaneous Settings ... 93
Status ... 96
Audit Log ... 97
Navigating to Audit Log ... 97

Viewing Audit Event Message Content ... 98
Viewing Audit Log Pagination Results ... 99
SMTP Event Notification Email and PHI ... 100
Working with Audit Log Results ... 101
Searching Audit Log Events ... 101
Sorting Audit Log Events ... 102
Filtering Audit Log Events by Date Range ... 103
Filtering Audit Log Events by Component ... 103
Pausing and Playing Audit Log Results ... 104
Accessing the Audit Log Configuration Settings ... 105
Working with General Settings ... 105
Working with Database Settings ... 106
Working with Notifications Settings ... 108
Working with Destinations Settings ... 109
Filtering Audit Events for Vocera Analytics ... 113
Using Audit Properties to Filter Events to Debug Log ... 113
Enabling and Disabling Filtering ... 114
Adapter Services ... 116
Monitoring Adapter Services ... 116
Starting and Stopping Adapter Services ... 117
Device Monitor ... 119
Working With Device Monitor ... 120
Uploading Device Logs ... 120
Database Cluster ... 122
Viewing Database Cluster Status ... 122
Failing Over and Repairing Database Clusters ... 124
Voice Cluster ... 126
Viewing Voice Cluster Status ... 126
Failing Over and Restarting Voice Cluster ... 127
Discovery Mode ... 128
Sequence of Failover Events ... 128
Badges and Clusters ... 129
Data Synchronization ... 129
Network Problems and Clustering ... 131
The Self-Healing Mechanism ... 132
Troubleshooting Network Problems and Clusters ... 133
Planned Network Outages ... 134
Geographically Distributed Clusters ... 134
Queues ... 137
Viewing Queued Message Detail ... 137
Canceling a Queued Message ... 138
Manage ... 139
Users ... 140
Searching for Users ... 141

Recommended Best Practices for Adding Users....142
Adding a User....143
Editing a User....154
Forwarding Calls....155
Adding Call Blocking Exceptions....156
Deleting a User....157
About Speech Recognition....158
The Dynamic Grammar....158
Grammars for Facilities....159
Homonym Recognition....161
Grammars for Facilities....161
Spoken Name Count....163
Intelligent Command Backoff....163
Offer to Learn a Name....164
Groups....166
Understanding Group Properties....167
Understanding Groups, Roles, and Policies....168
Designating Group Types....168
Default Groups....169
Adding a Group....170
Editing a Group....173
Granting Voice Permissions....174
Group Managers and Device Managers....184
Deleting a Group....185
Facilities....186
Adding a Facility....186
About Global Facility....191
About Users and Telephone Numbers....192
Access Code Exceptions....193
Toll Exceptions....194
Direct Inward Dialing....194
Telephony PINs....196
Dynamic Extensions....198
Shared Telephony Configuration....199
Initiating Emergency Broadcasts Silently....201
Playing with Easter Eggs....201
Editing a Facility....202
About Departments, Rooms, and Beds....206
Working with Departments....207
Working with Rooms....211
Working with Beds....216
Deleting a Facility....221
Contacts....222
Adding a Contact....223
Editing a Contact....225

Deleting a Contact....226
About Contacts List for the Global Facility....226
Using Voice Commands with Contacts....227
Using Macros in Contacts....227
Calling Home....227
Night-Bell Pickup....227
Access Point (AP) Locations....228
Defining Locations....228
Managing Access Point Locations....229
Adding an Access Point Location....229
Editing an Access Point Location....230
Deleting an Access Point Location....231
Searching for AP Locations....231
Recording a Location Name....232
Using Voice Commands to Assign Access Points....233
Device Inventory....234
Adding a Device....234
Editing a Device....236
Filtering Devices by Facility....237
Sorting Devices....237
Searching for Devices....238
Viewing Devices....238
Deleting a Device....239
Device Management Guidelines....239
Enterprise Guidelines....239
Group Guidelines....240
Managing Shared Devices....240
Device Management Roles....240
System Device Manager Responsibilities....241
Group Device Manager Responsibilities....241
Device Management Capabilities per Role....242
About Serial Numbers and MAC Addresses....242
Using a Barcode Scanner to Add Devices....243
Tips for Scanning Devices....244
Barcode Scanner Requirements....244
Adding Devices Using a Barcode Scanner....245
Automatically Loading Devices into the System....245
Labeling Devices....246
Monitoring Active Devices....246
Reporting on Devices....247
Device Management Licensing....247
Templates....248
Adding a Template....249
Editing a Template....252
Deleting a Template....253

Bulk Actions ... 254
Importing Data to the System ... 255
Exporting Data to a CSV File ... 257
Importing Text into Microsoft Excel ... 258
Template Reference ... 259
The Facilities Template ... 259
The Groups Template ... 260
The Users Template ... 265
The Group Members Template ... 268
The Access Point Locations Template ... 269
The Access Points Template ... 269
The Contacts Template ... 270
The Beds Template ... 273
The Devices Template ... 274
The Assignment Locations Template ... 275
The Assignment Roles Template ... 275
The Templates Template ... 276
The Template Sharing Template ... 279
The Template Selected Group Template ... 279
Settings ... 280
System Configuration ... 281
General Configuration ... 281
Setting System Preferences ... 283
Working with Favor Frequently Called for Users and Departments ... 284
Setting Sweep Options ... 286
Viewing Device Information Statuses ... 286
Adding a Device Status ... 288
Editing a Device Status ... 288
Reorder Device Status Values ... 289
Delete Device Status Values ... 289
User Defaults ... 291
Overriding User Settings ... 291
Specifying Genie Settings ... 291
Specifying Notifications and Miscellaneous Settings ... 293
Specifying Initial Passwords ... 296
Adapters ... 298
Accessing the Adapters List ... 298
Viewing Adapter Configuration Details ... 300
Creating a New Adapter ... 301
Uploading a Bundle ... 302
Datasets ... 305
Accessing the Datasets List ... 305
Viewing Dataset Configuration Details ... 306
Creating a New Dataset ... 307

Workflows....309
Accessing the Workflows List....309
Configuring the Workflows Settings....310
Managing Workflows....311
Creating a New Workflow....312
Editing a Workflow....313
Testing a Workflow....314
Cloning a Workflow....315
Removing a Workflow....316
Working With Workflow Pages....317
Creating a New Page....318
Editing a Page....319
Cloning a Page....320
Removing a Page....321
Network Settings....324
Static or Dynamic IP Address Settings....325
Editing Network Settings....325
Selecting a Date and Time Format....327
Configuring System Date and Time....327
Voice License....329
Platform License....331
System Backups....332
Accessing the System Backups List....333
Understanding Database Optimization....334
Configuring a Database Optimization Schedule....334
Understanding Manual System Backups....335
Creating a Manual Backup....335
Understanding a System Backup Restore....336
Uploading a Saved Backup....337
Downloading a System Backup....337
Restoring a System Backup....338
Viewing Compatibility Issues....340
Understanding the Automatic Backups....341
Configuring the Automatic Backup General Settings....344
Configuring an SMB Transfer of a Backup....345
Configuring an FTP Transfer of a Backup....346
Understanding SFTP Transfer of a Backup....346
Understanding the Transfer of a Backup to a Secondary System....348
High Availability....351
Understanding Clustering....351
Cluster Management Tips....351
Configuring Clusters....352
Enabling Clustering on a Standalone Server....352
Joining a Database Cluster....354

Changing the Failover Sequence....355
Removing a Node from a Cluster....355
Accessing Remote Support in a Cluster....356
Cluster Email Notifications....357
Cluster Health Checks....357
F5 BIG-IP Health Check Configuration for a Cluster....358
Example Configuration for Vocera Platform and an ADC....359
HA Deployment Configuration Selection....362
Layer 2 Adjacent Deployment Model....363
Third-Party Load Balancer (Non-Layer 2 Adjacent) Deployment Model....363
FAQs for HA Decisions....364
Why do I need a VIP in my facility?....364
What are the network requirements for the non-ADC deployment model?....364
Why can't the non-ADC model be deployed across two different data centers with different subnets?....364
How can I support a multiple data center deployment without Ethernet Layer 2 Adjacency between them?....364
How do I span Layer 2 Adjacency across the data centers?....365
Can a third element manage the public VIP when nodes are on two different subnets?....365
Can the Vocera Platform support my ADC?....365
When our facility is not using an ADC, can I determine when an adapter and/or the system is performing as expected?....365
When our facility is using an ADC (load balancer), can I determine when the master is available and responding as expected?....366
What is the failover time?....366
Will any of my data be lost during a failover?....366
Badge Properties Editor....367
Using the Badge Properties Editor....367
B3000 Badge Properties Configuration....368
B3000N Badge Properties Configuration....373
V5000 Smartbadge Properties Configuration....379
Configuration Packages....384
About the Core Configuration Packages....384
About the Supplementary Configuration Packages....385
Working with Configuration Packages....386
Installed Software....388
Security....389
Authentication....390
Configuring Authentication Settings....391
Using a Keytab File for Kerberos Authentication....394
Certificates....397
Uploading a Certificate....397
Security Policies....399
Accessing Security Policies....399
Default Security Policy....400
Creating a Security Policy....401
Editing a Security Policy....402
Removing a Security Policy....403

Understanding Security Policy Items....404
Console Session Timeout Policy Item....404
Console Access Management Policy Items....405
Maximum File Size of a User's Profile Photo Policy Item....406
Mobile Client Security Policy Items....406
Password Authentication Policy Items....407
PIN Authentication Policy Items....409
Staff Assignment All Department Access Policy Item....410
Vocera Vina Policy Items....411
Managing Security Policy Items....413
Adding a Policy Item....413
Editing a Policy Item....414
Removing a Policy Item....415
Roles....417
Accessing Roles....418
Adding a Role....418
Associating Roles with Groups....420
Editing a Role....420
Removing a Role....421
Remote Support....423
Establishing a Remote Session....424
Disconnecting a Remote Session....425
My Workflow....426
About the Vocera Platform My Workflow Guide....427
The My Workflow Home Screen Layout....428
Matrix of Workflows and User Roles....429

Getting Started

This section provides an overview of the Vocera Platform and describes how to use the Vocera Platform Web Console and the documentation.

- About the Vocera Platform on page 13
- About the Vocera Platform Administration Guide on page 14
- Related Documentation on page 15
- Using the Vocera Platform Web Console on page 16

About the Vocera Platform

The Vocera Platform optimizes patient safety by helping clinicians make real-time decisions and communicate instantly in critical situations; it is the intelligent ecosystem that connects all the people and information needed to deliver patient care.

With the intelligence of the Vocera Platform, clinicians can quickly determine what to prioritize next and close the loop faster with secure messaging, phone calls, and alert and alarm notifications--all in one place. You can locate people quickly, collaborate productively, and reduce the noise, using the device that fits your workflow--the Vocera Vina smartphone app, the V-Series Smartbadge, or the B-Series Badge. The Vocera Platform enables the flow of meaningful, actionable information between people and systems and allows it to be received when, where, and how it's needed, keeping the patient at the center of care.

In addition, the Vocera Platform now offers simplified deployment, maintenance, and administration, as well as a smaller footprint requiring fewer servers.

About the Vocera Platform Administration Guide

The Vocera Platform Administration Guide describes how to perform tasks using the Vocera Platform Web Console.

You can use this document as you work with the Vocera Platform Web 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 Vocera Platform Web Console.

Related Documentation

This section includes a list of recommended reference documents that support the Vocera Platform Administration Guide.

- Vocera Platform Installation Guide — Describes the install and upgrade guidelines for the Vocera Platform.
- Vocera B-Series Badge User Guide — Describes the usage guidelines for your Vocera Badge and supported features.
- Vocera V-Series Smartbadge User Guide — Describes the usage guidelines for your Vocera Smartbadge and supported features.
- Vocera Vina User Guide — Describes the usage guidelines for your Vocera Vina application and supported features.
- Vocera Voice Commands Reference Guide — Describes supported Vocera voice commands and guidelines to use these commands on your Vocera Badges, Vocera Smartbadges, and smartphones.

Using the Vocera Platform Web Console

The Vocera Platform Web Console is a browser-based application that allows you to establish default behavior, define system entities such as users and groups, specify workflows, and configure other custom settings for your Vocera Platform.

About Vocera Platform Web Console

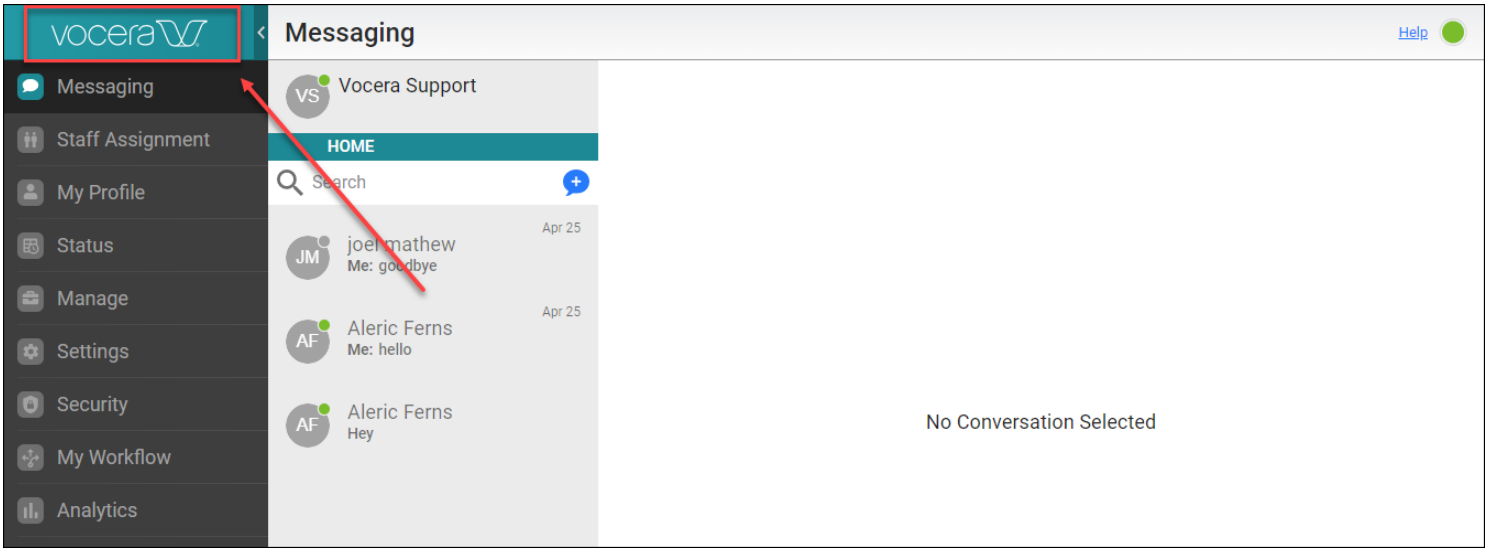
The Vocera Platform Web Console is a browser-based application that provides a graphical user interface for users to establish default behavior, define system entities such as users and groups, specify workflows, and configure other custom settings for the Vocera Platform.

The Vocera Platform Web Console is an integrated web based application that unifies the capabilities of Vocera Platform Voice Service along with the Vocera Platform Messaging, and Vocera Platform Staff Assignment.

Depending on the role associated with your account, you can access and use the Vina Web, Vocera Platform Staff Assignment, or Vocera Platform My Profile applications from the Web Console

After you login to the Web Console you can click through the user interface to performs various tasks.

To hide the left navigation bar, click the expanded Vocera logo.



If the left navigation bar is hidden, click the Vocera logo again to expand it and view the sections.

Browser Requirements

The Vocera Platform Web Console supports most popular web browsers. This section lists the specific browsers and versions that have been tested.

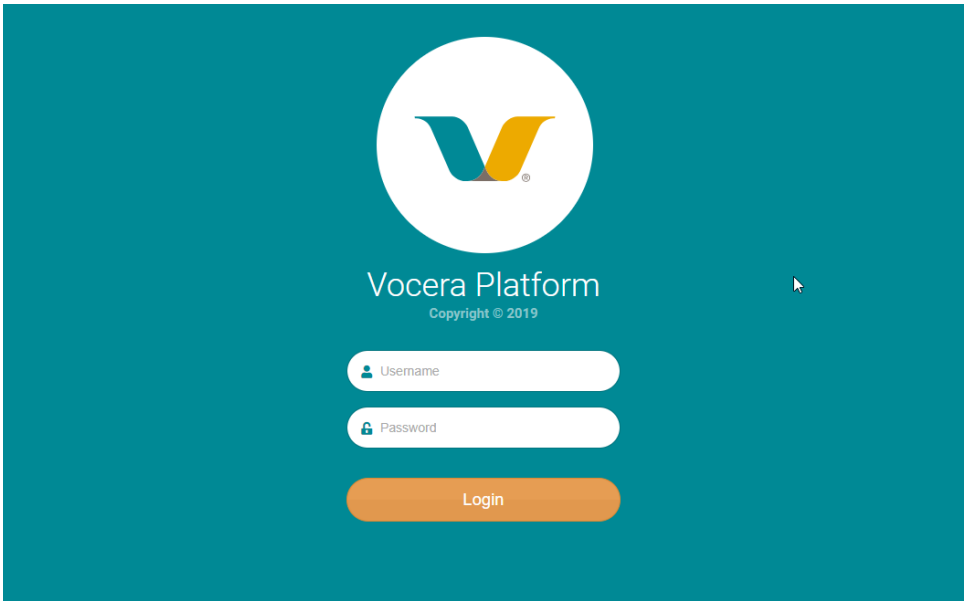
Browser	Version
Apple Safari	Version 10.10 or later
Google Chrome	Version 65 or later
Microsoft Internet Explorer	Version 11 or later
Microsoft Edge for Windows 10	Version 17 or later
Mozilla Firefox	Version 58 or later

Logging Into the Vocera Platform Web Console

You can typically log into the Vocera Platform Web Console using the credentials you provide for other applications in your organization (your Active Directory credentials).

Use the following steps to log into the Vocera Platform Web Console using Active Directory authentication:

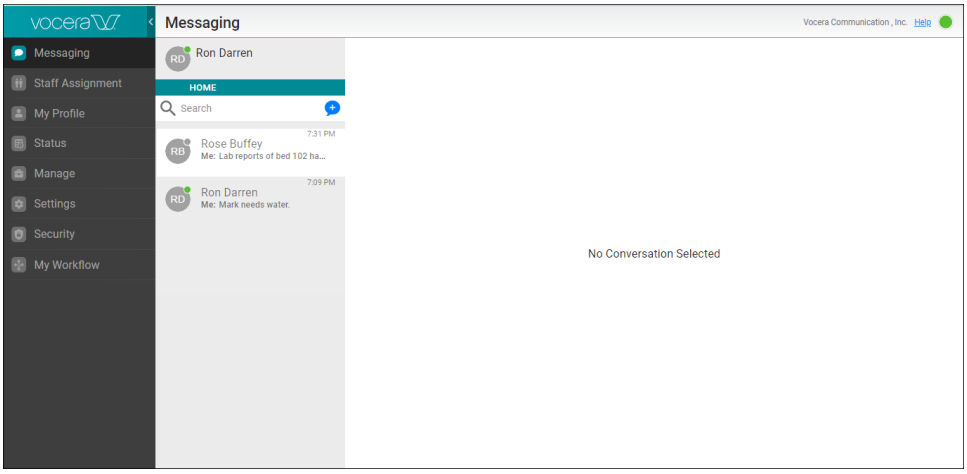
1. In your browser, type the URL of the Vocera Platform Web Console that your administrator has provided for you.
   The Vocera Platform login screen appears.



2. Specify the following values:

Field	Description
Username	Enter your username (up to 250 characters).
Password	Enter your password (up to 127 characters).

3. Click **Log In**.
   The Vocera Platform Web Console screen appears.

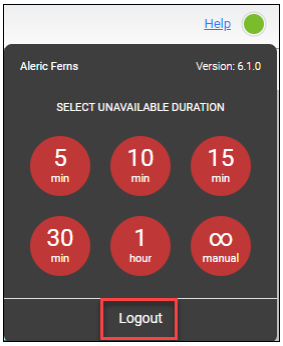


Logging Out

When you are finished using the Vocera Platform Web Console, log out.

To log out from the Vocera Platform Web Console:

1. Click the presence icon in the top right corner of the Vocera Platform Web Console.
   The presence dialog box appears.



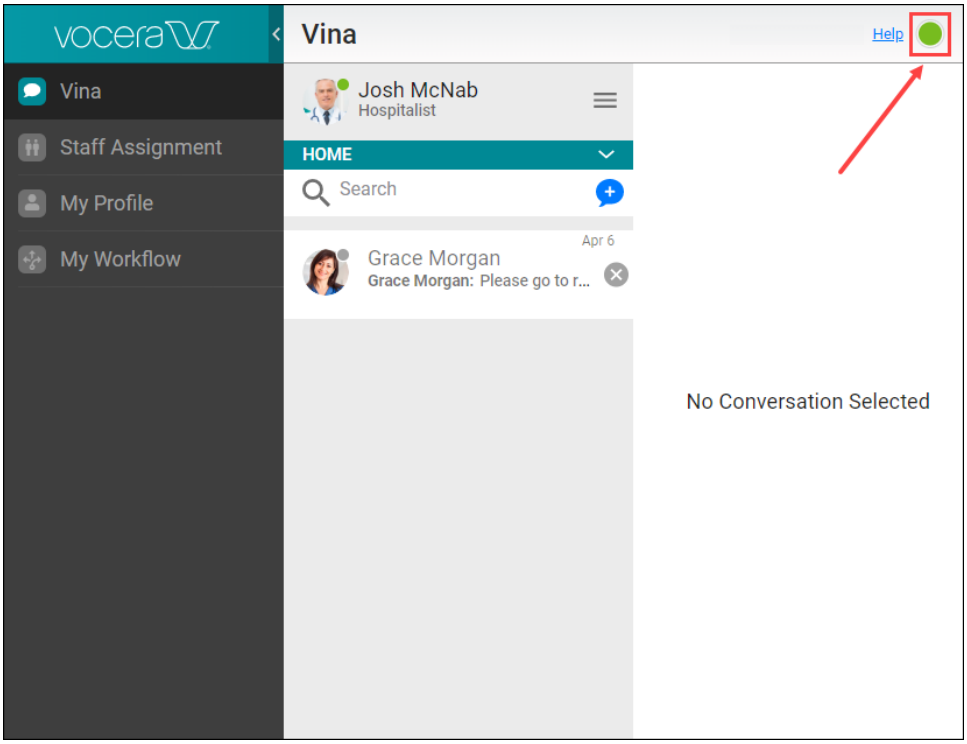
2. Click **Logout** at the bottom of this dialog box.
   The system logs you out.

Setting Presence and Availability

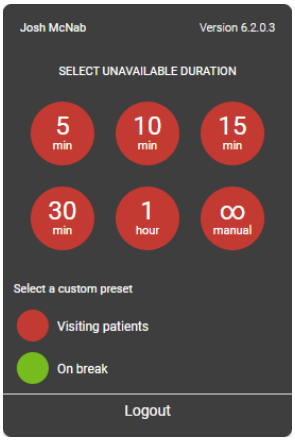
You can specify that you are unavailable, either for a specified period of time or until you make yourself available again.

To specify a period of time in which you are unavailable

1. Click the presence icon at the top right corner of the Home screen, as shown in the following screenshot.



   A popup menu appears, displaying a list of options to select.



2. Select one of the following:
   - Cick one of the options in the **Select unavailable duration** section to specify that you are unavailable for a predefined period of time. After this time has elapsed, you are listed as available.
   - Click **Manual** to specify a custom unavailability interval. You remain unavailable until you make yourself available again.
   - Click on one of the options in the **Select a custom preset** section. The custom preset feature is available only if this feature is enabled by your system administrators.

When you have specified an unavailability interval, the presence icon turns red indicating a DND or unavailable status.

You can click the red presence icon again to revert back to an avaialble status indicated by a green color.

Messaging

This section provides an overview of the Vina Web module.

- About the Vocera Vina Web User Guide on page 22
- About Conversations on page 23
- About Templates on page 38
- About Personal Messages on page 43
- About Mass Notifications on page 44
- About Favorites on page 45
- Personal Titles on page 48

About the Vocera Vina Web User Guide

The Vocera Vina Web User Guide describes how to perform tasks using the Vina Web.

You can use this document as you work with the Vina Web, 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 Vina Web.

About Conversations

When you start Vina Web, the Home screen displays a list of the conversations and group chats that you have participated in. You can use messaging and chat-style conversations to communicate with other users in your network.

You can:

- Start a conversation with another user.
- Start a group chat with multiple users.

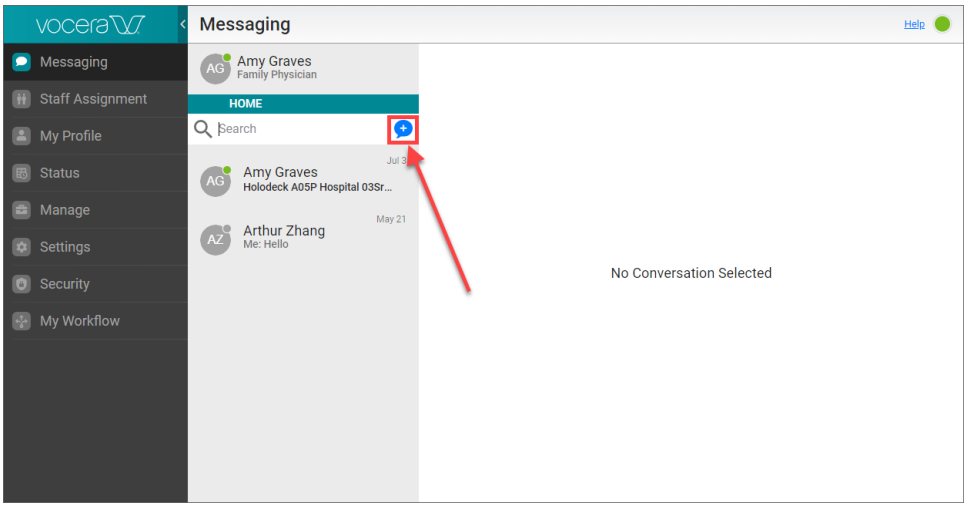
Note: Your administrator may have defined the maximum number of conversations or group chats that can appear on your screen. Contact your administrator if you have any concerns about this.

Note: You can miss a message if it is sent in a conversation or group chat that has scrolled off your screen.

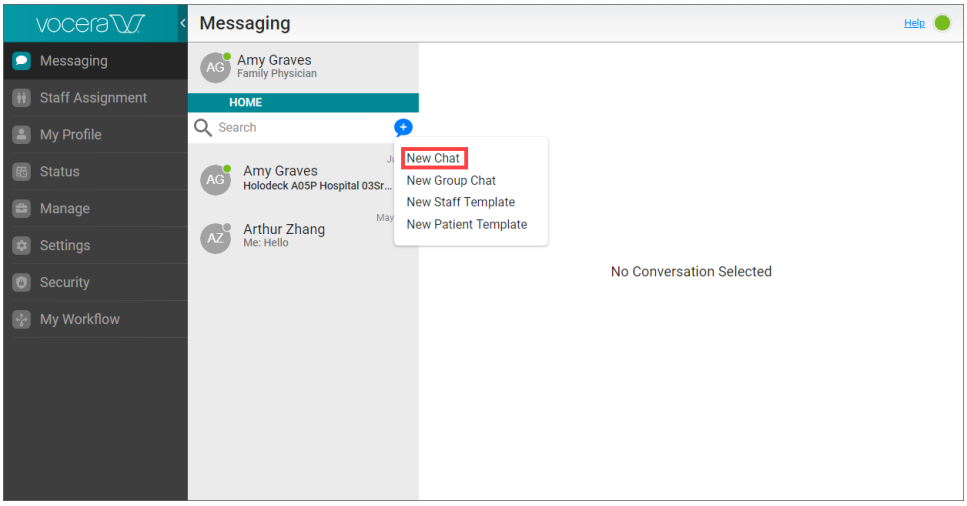
Starting a Conversation

From the panel that displays the list of conversations, you can start a new conversation.

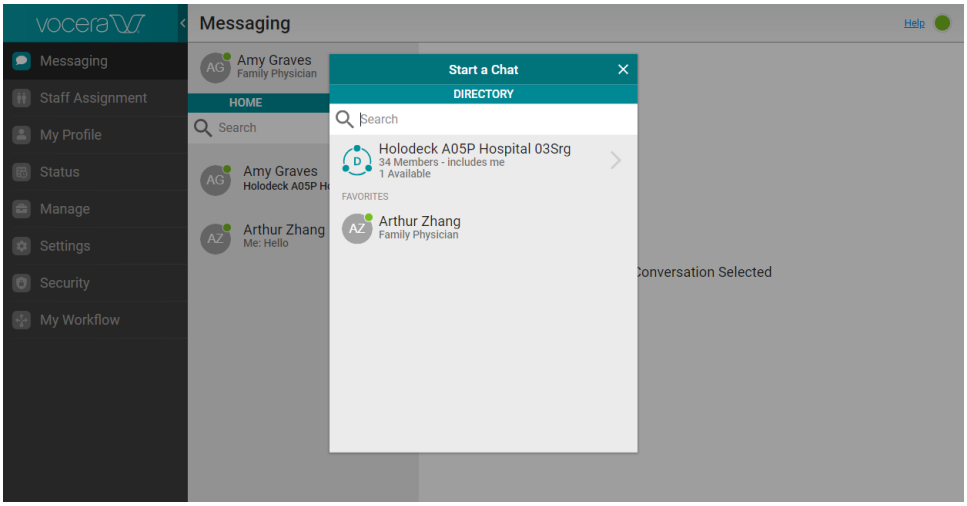
1. In the panel that displays the list of conversations, click the **New** icon.



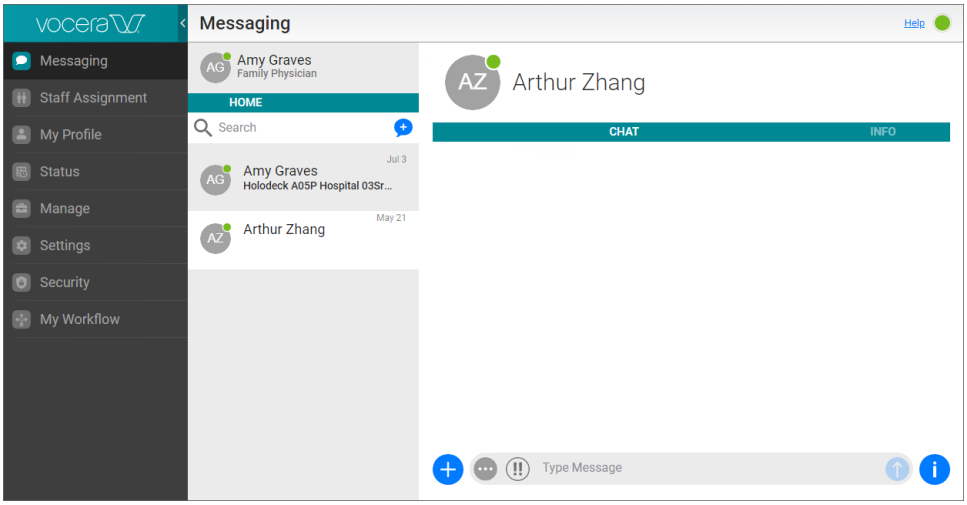
2. From the pop-up menu that appears, select **New Chat**.



The Start A Chat panel appears.



3. In the Start A Chat panel, select the contact with which you want to have a conversation:
   a. If the contact is defined as a favorite, click the link for that contact to start the conversation. (See About Favorites on page 45 for more information on Favorites.)
   b. If the contact is a member of a group, click the group to display the contacts that are members of the group, then click the member to start the conversation.
   c. In the Search field, type text consisting of some or all of the contact's name. All contacts matching this search text are displayed. Click the entry for the contact with which you want to start a conversation.
4. When you have selected a message participant, the chat screen appears.



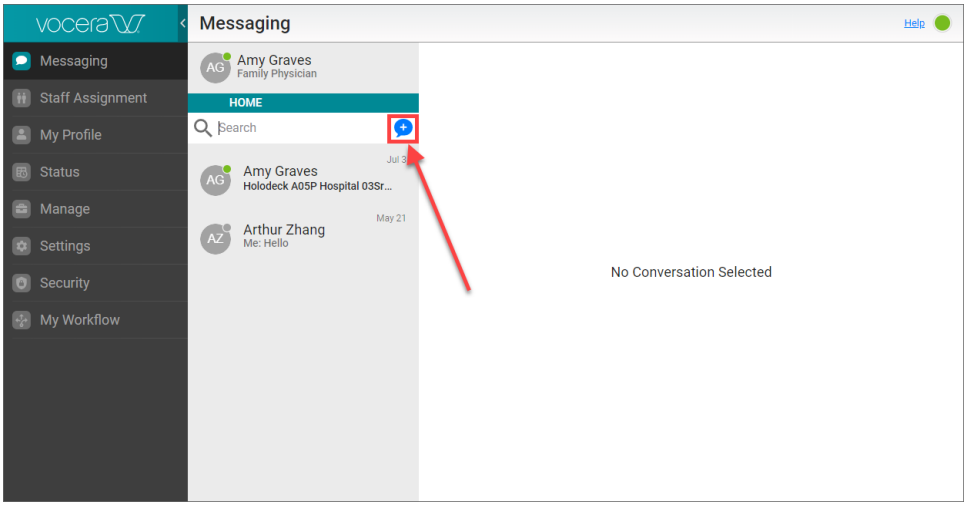
In the Chat screen, you can start the conversation. See Adding a Message on page 28 for information on how to do this.

If you have previously started a 1-on-1 conversation with this contact, the existing conversation is rejoined. Conversations that are between more than two users or contain a patient reference are always new conversations.

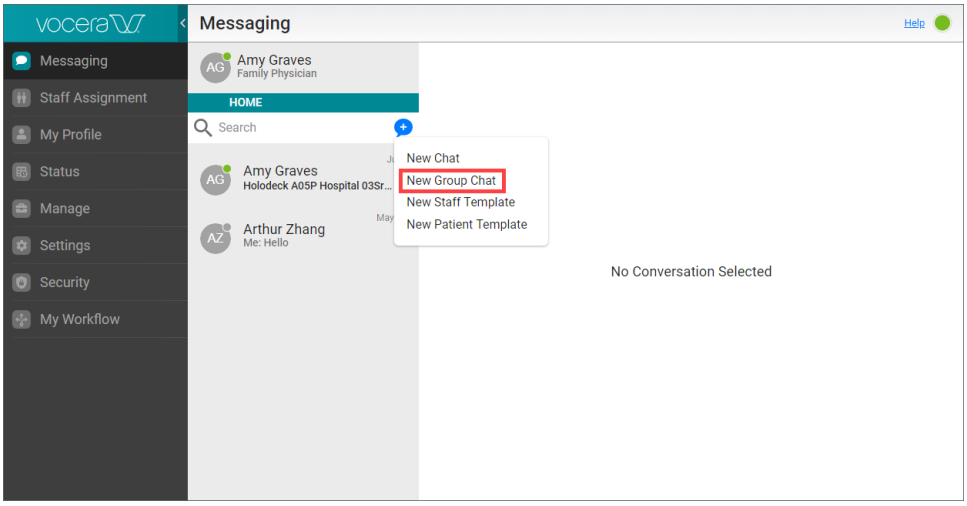
Starting a Group Chat

You can start a group chat with the members of a group to which you belong.

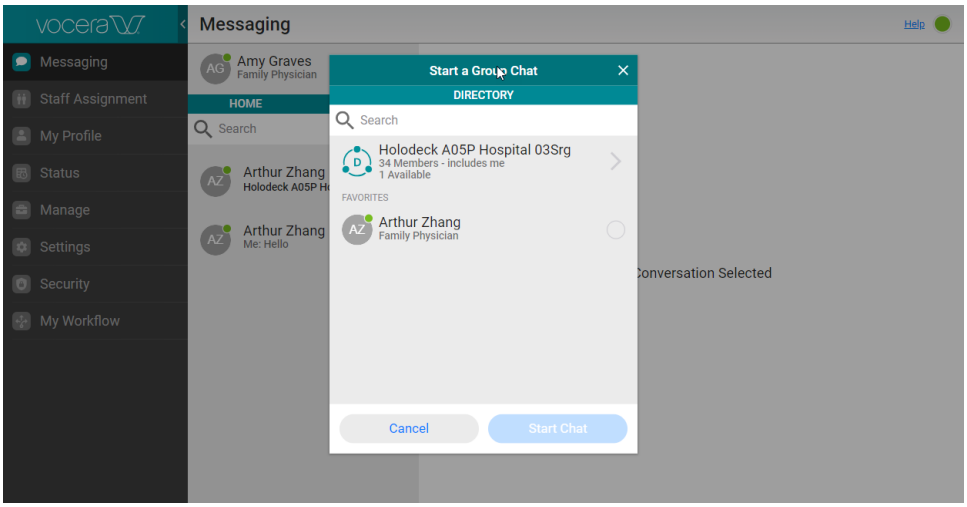
1. In the panel that displays the list of conversations, click the **New** icon.



2. From the pop-up menu that appears, select **New Group Chat**.



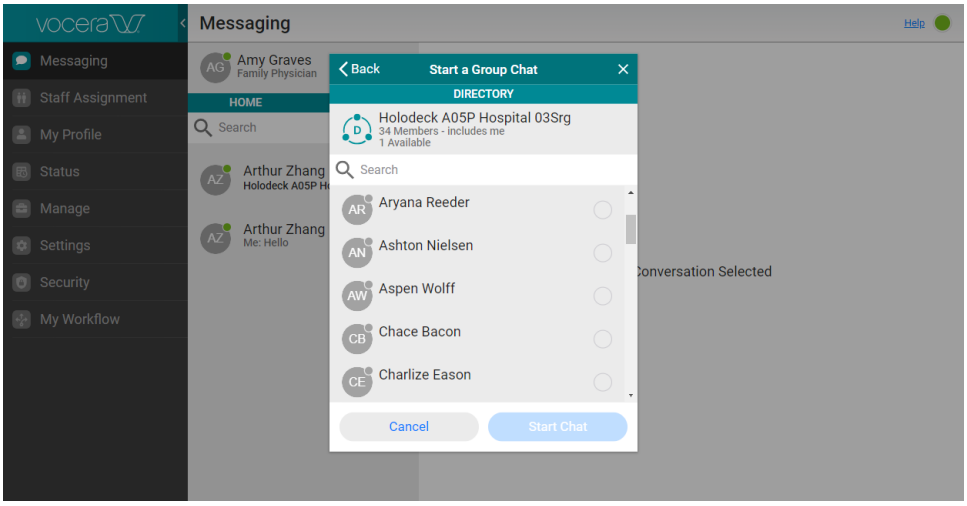
The Start A Group Chat panel appears.



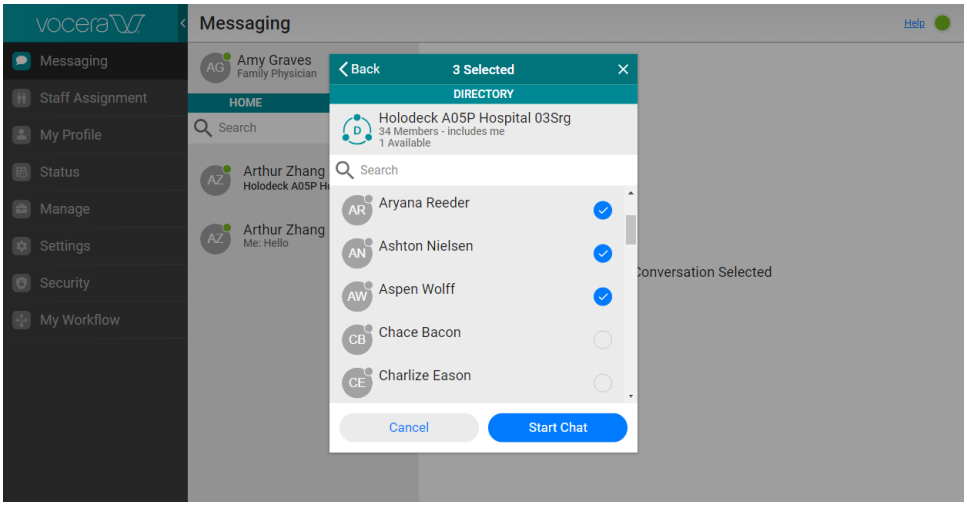
From this panel, shortcuts are defined when you right-click on a group, a department or an individual user that may allow you to send a message or update your favorites list.

- If you right-click on a group, you can select **Message Group** to send a message to the entire group. If the group is not a favorite, select **Make Favorite** to make this group a favorite. If the group already is a favorite, select **Remove Favorite** to remove the group from your favorites list.
- If you right-click on a department, you can select **Message Department** to send a message to the entire department.
- If you right-click on a user, and the user is not a favorite, select **Make Favorite** to make this user a favorite. If the user is a favorite, select **Remove Favorite** to remove the user from your favorites list.

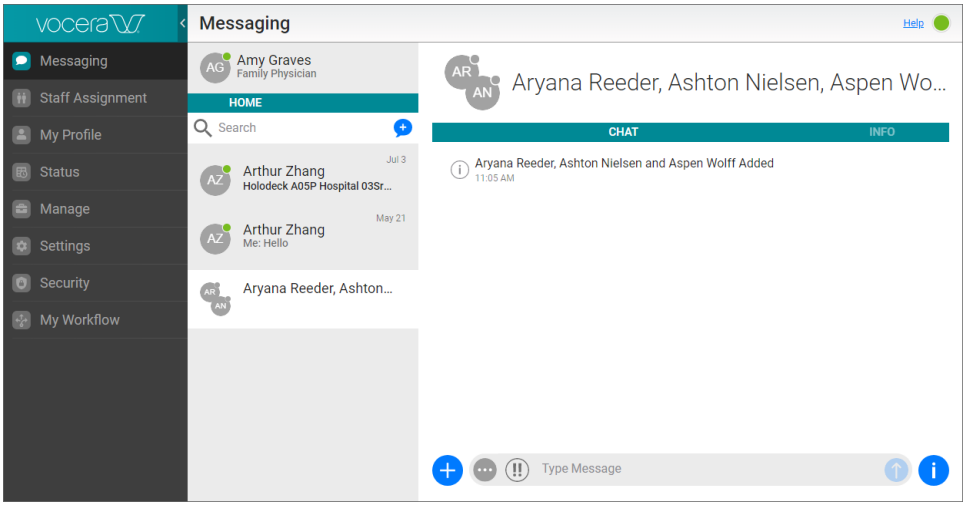
3. Tap the name of a group. A list of the group members appears.



4. Use the checkboxes at the right to select the members of the group with which you want to chat.
5. Click **Start Chat** to start the group chat.



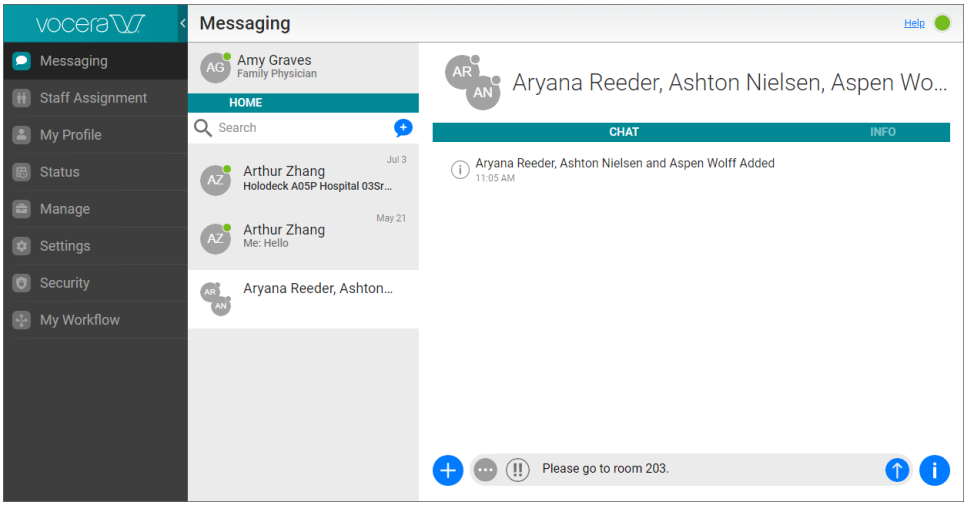
The Vina Web creates a chat room in which the selected members of the group are invited to be participants.



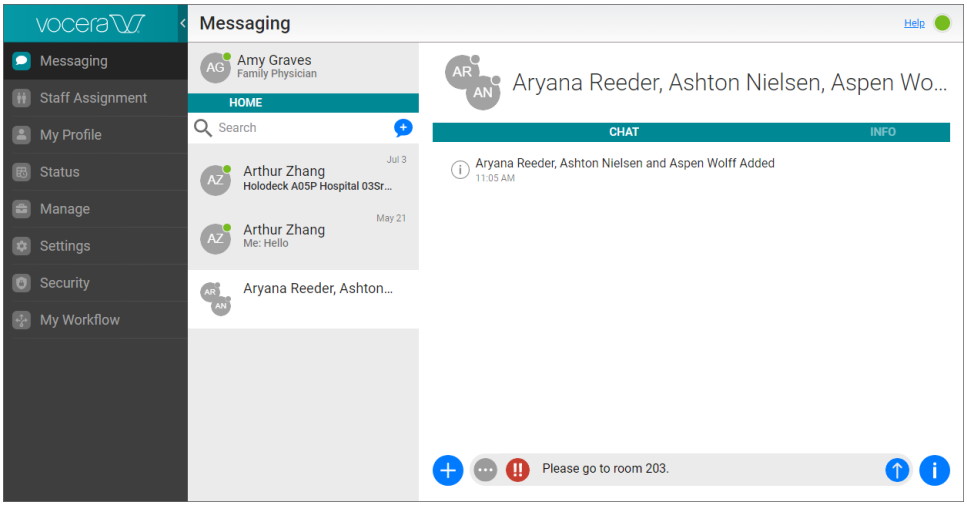
Adding a Message

You can add a new message to a conversation or group chat that you are in.

1. To send a message, type the text in the field at the bottom of the screen.

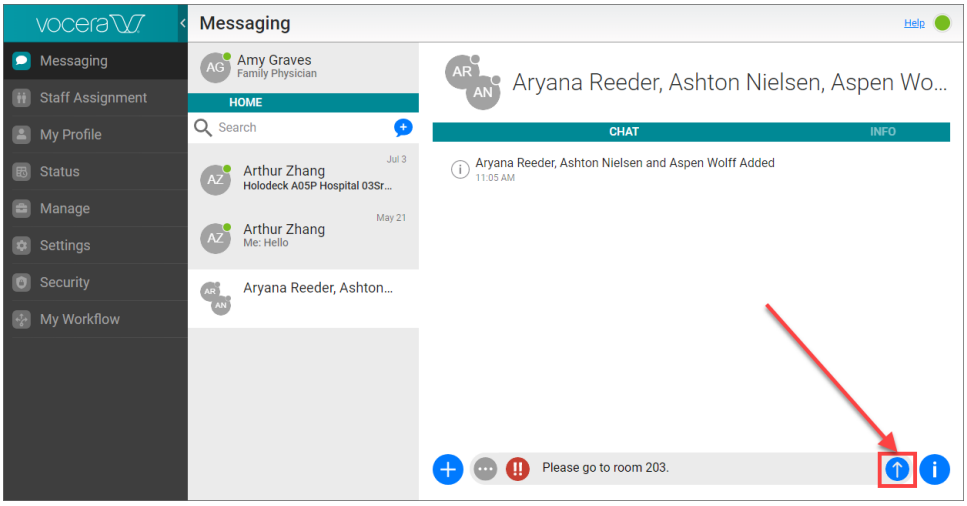


2. To ask for an acknowledgment to your message, click the exclamation marks icon located to the left of the text.

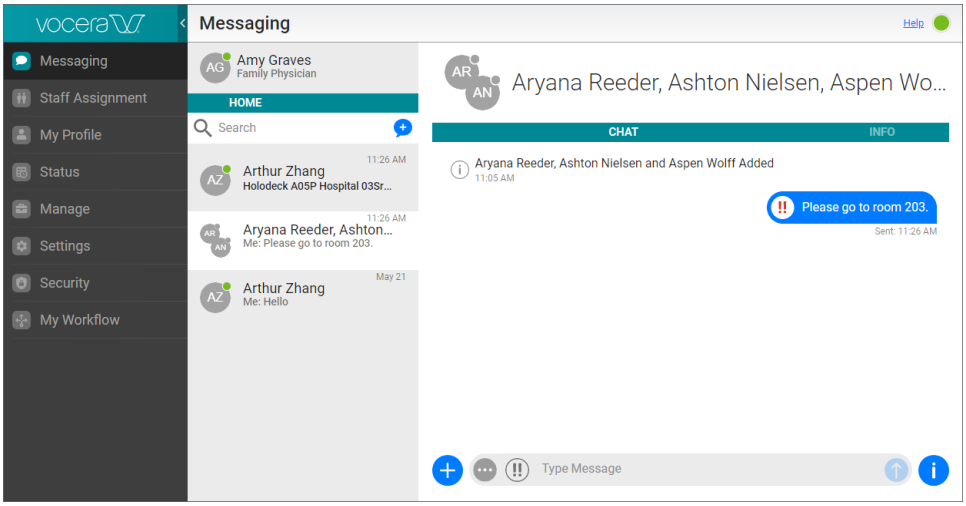


   This is a convenient way to mark message text as high priority and ensure that it is acknowledged and not just read.

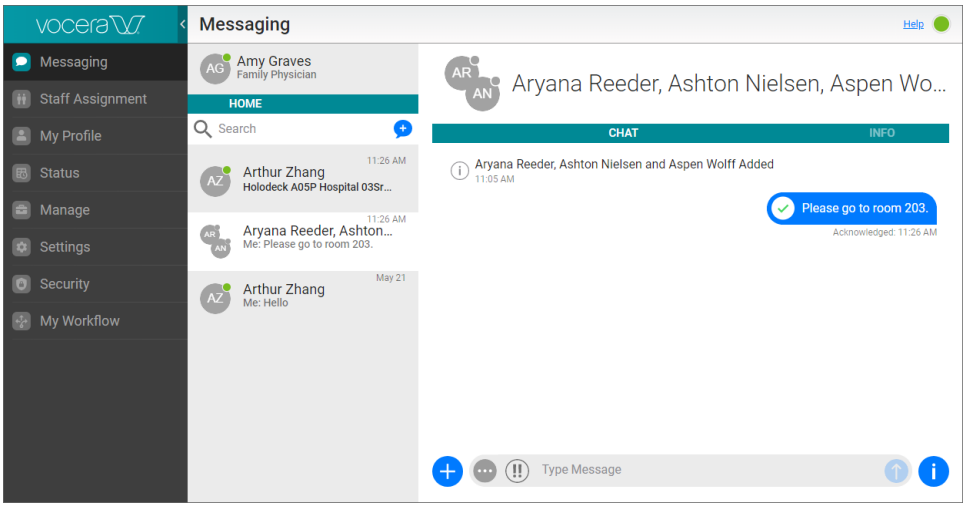
3. Click the Send icon to send the message. This icon is located at the bottom right of the screen.



The sent message appears on the screen of all other participants in the conversation or group chat. If you have sent a message that requires an acknowledgement, the screen indicates this.



If the message has been acknowledged by all participants, a checkmark icon appears.



For a complete list of all possible statuses for sent and received messages, see Message States on page 30.

Message States

Each sent message in a conversation or group chat displays a message state that is based on the current users and the most recent received delivery information. Each received message indicates whether you have read or acknowledged it.

Each sent message displays one of the following message states:

State	Description	Timestamp Shown
<None>	Message sent, but no received response from the server.	<None>
Failed	Not received by server. The client has disconnected or 20 seconds have elapsed.	Time the failure was detected
Sent	Received by the server in a conversation or chat.	Time the server received the message
Delivered to some	No one has read or acknowledged the message. Some of the users have received the message, but not all.	Most recent received time
Delivered	No one has read or acknowledged the message. All users have received the message.	Most recent received time
Read by some	No one has acknowledged the message. Some of the users have displayed the message, but not all.	Most recent displayed time
Read	No one has acknowledged the message. All users have displayed the message.	Most recent displayed time
Acknowledged by some	Some of the users have acknowledged the message but not all.	Most recent acknowledged time
Acknowledged	All of the users have acknowledged the message.	Most recent acknowledged time

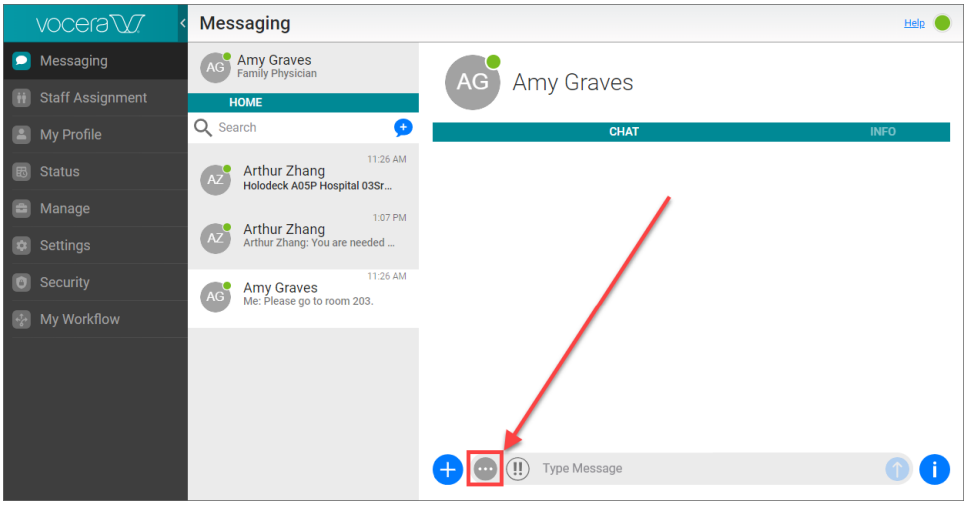
Each received message displays one of the following states:

State	Description	Timestamp Shown
Received	The message has been received, but the entire message has not been displayed on the screen.	N/A
Read	You have read the message.	The time that you read the message
Acknowledged	You have acknowledged the message.	The time that you acknowledged the message.

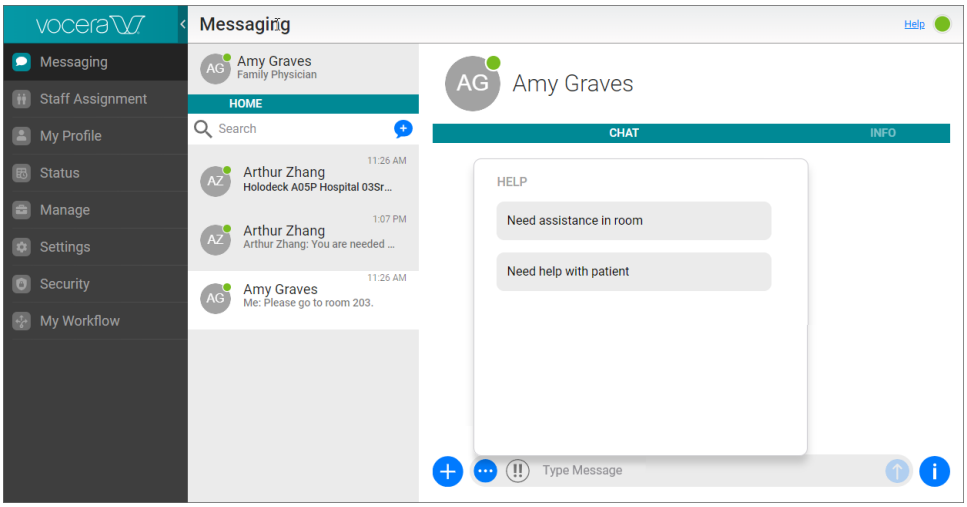
Sending a Quick Response

Some of the messages that are most frequently used in a conversation or group chat are available in a menu for easy access. This enables you to send a quick response when you receive an urgent message.

1. To send a quick response in a conversation or group chat, tap the Quick Message icon.



2. Choose a quick response from the list that appears.



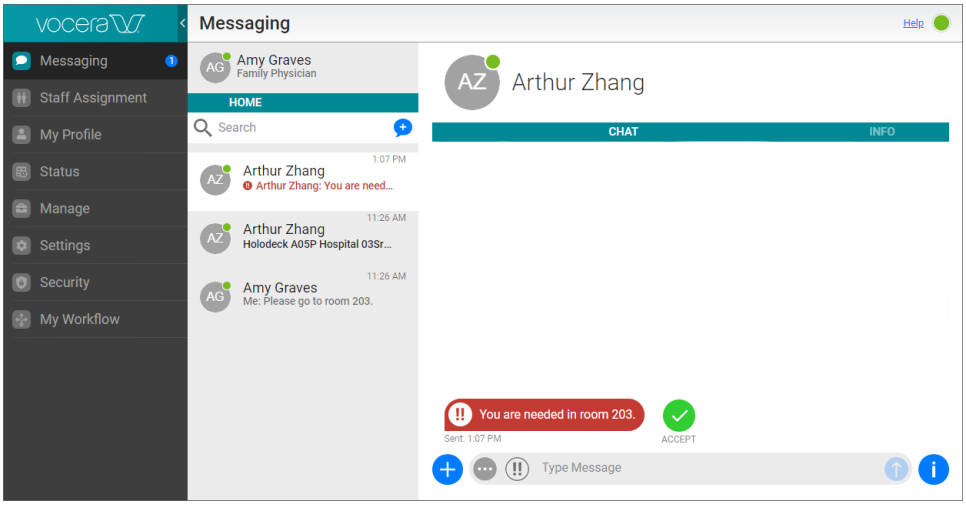
The quick response appears in your conversation.

Your administrator may have organized the available quick responses into convenient categories, such as Product Quick Response, Requests, and Status Update. This makes it easier for you to locate the appropriate message.

Acknowledging a Message

You may be sent a message that requires you to acknowledge to the sender that you have seen it.

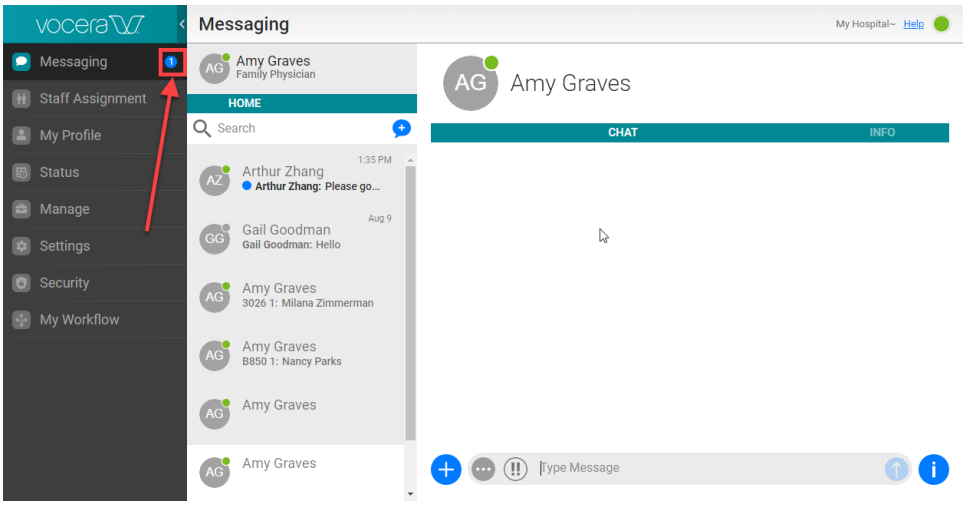
If you receive a message that requires acknowledgment, it is displayed with a red background:



Click **Accept** to acknowledge the message.

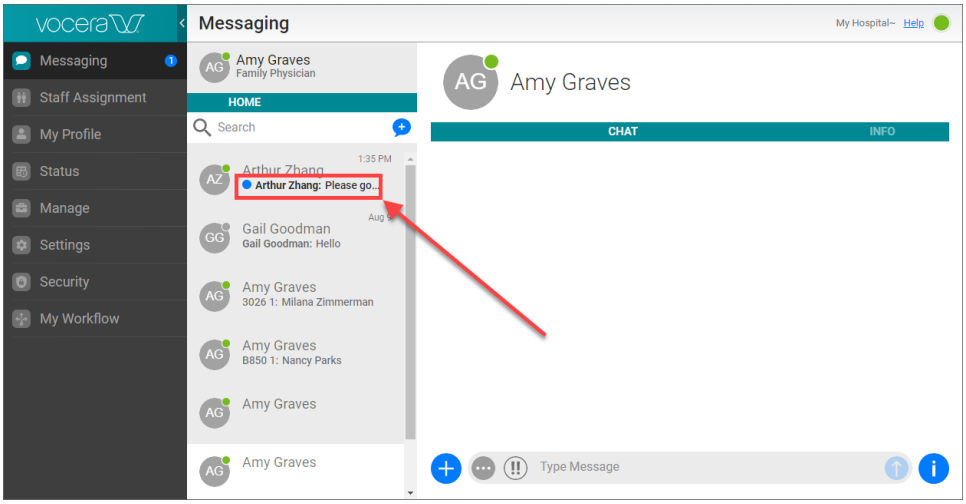
Conversations with Unread Messages

If you have any active conversations that contain messages that you have not read, a number appears next to the Messaging link in the left pane.



The number next to the Messaging link is the number of conversations containing unread messages, not the total number of unread messages.

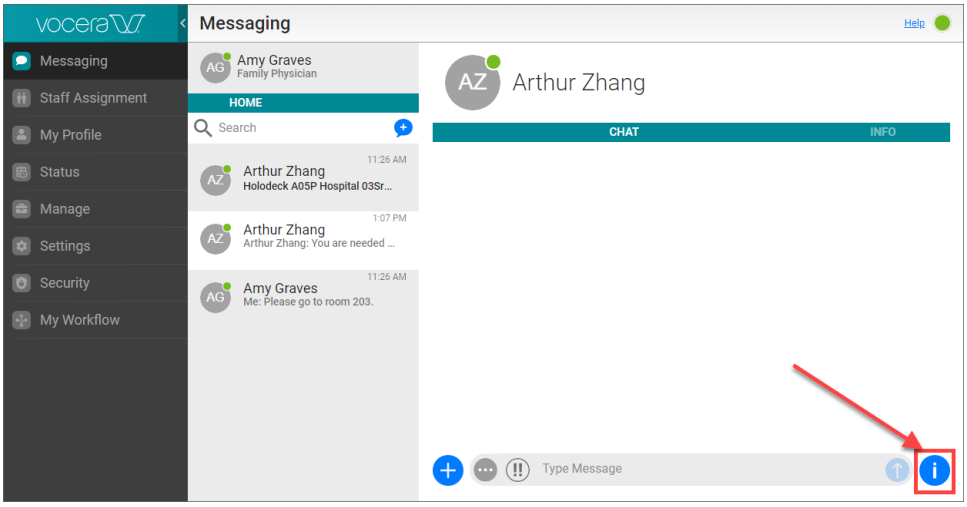
In the list of conversations, the conversations that contain unread messages have their last message displayed in bold.



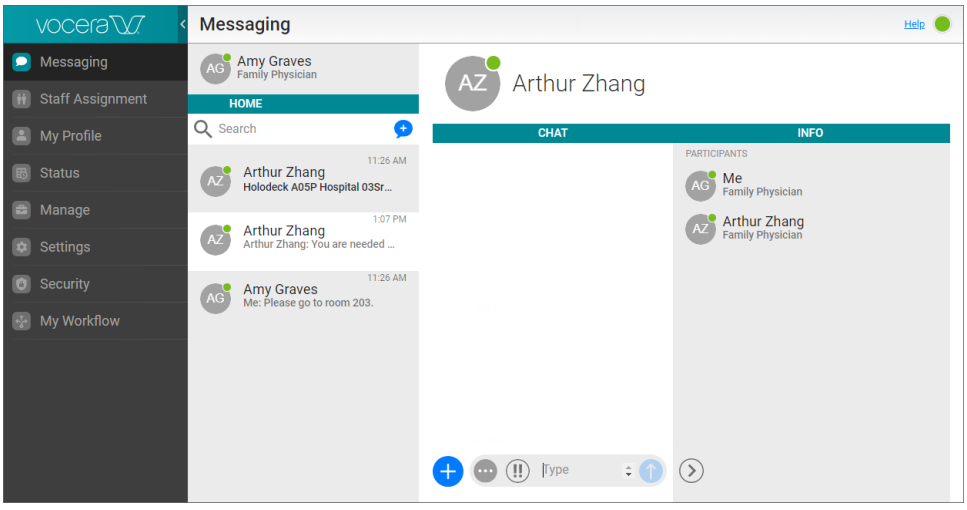
Viewing Participants

You can view the list of participants in any conversation or group chat.

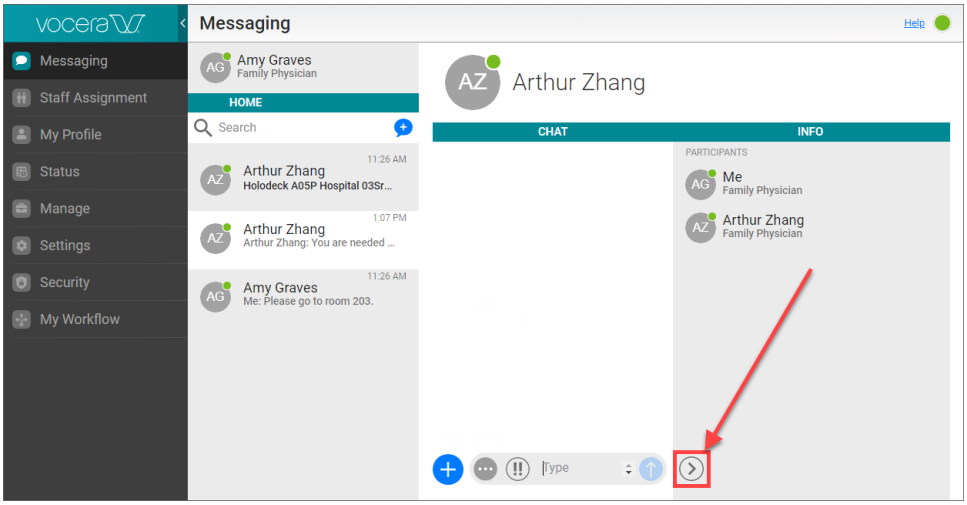
1. In your conversation or group chat, click the Info link at the bottom right.



A list of the participants appears.



2. Click the Back link to hide the list of participants.

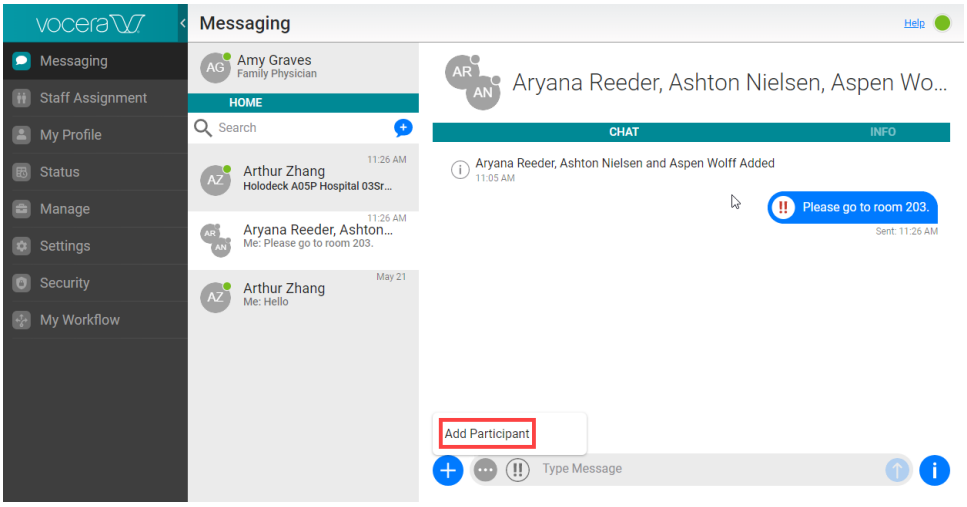


Adding a Participant to a Conversation

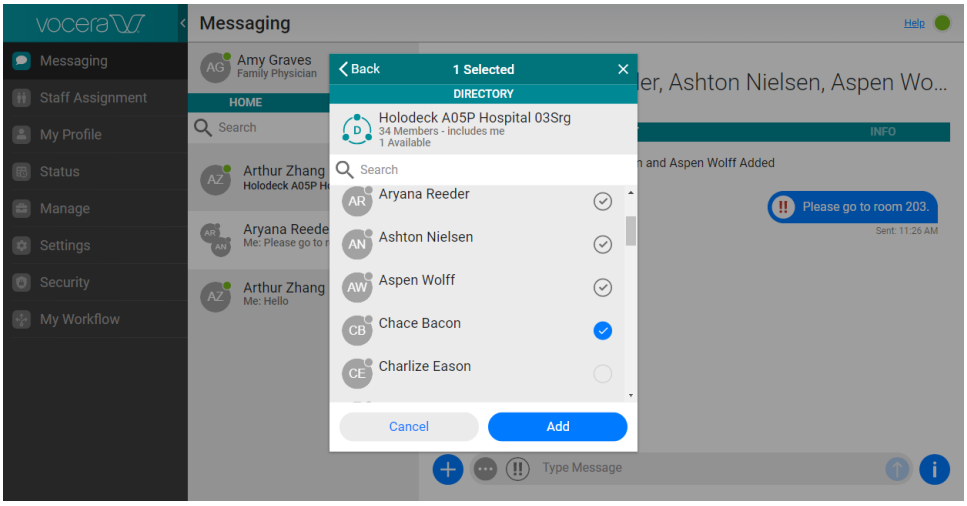
If you are in an existing group chat, you can add another participant to it. If you are in a conversation with one other person, and you want to add a participant, you can create a new group chat consisting of you, the other person in the conversation, and the new participant.

Note: The maximum number of participants in a conversation is 50.

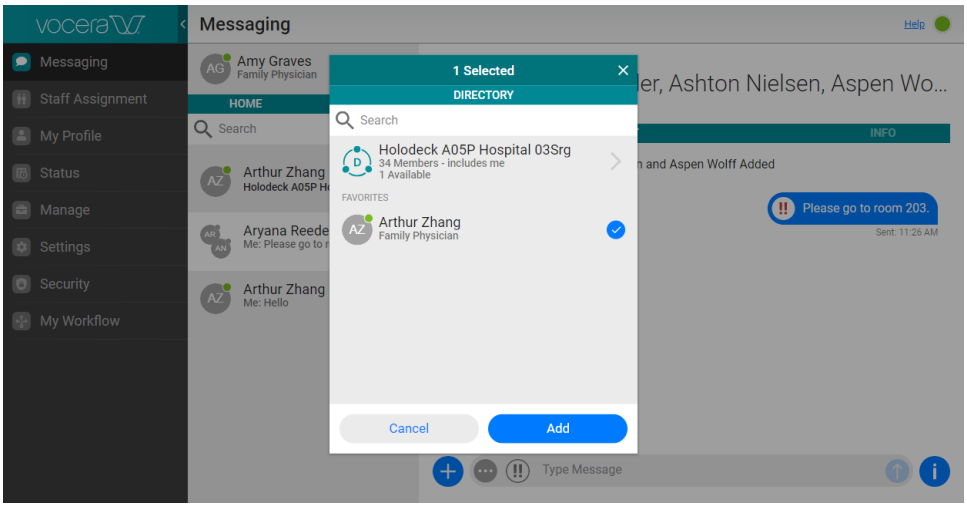
1. In your conversation or group chat, click the Add link at the bottom left. From the popup menu that appears, select **Create Group Chat** if you are in a conversation, or select **Add Participant** if you are already in a group chat.



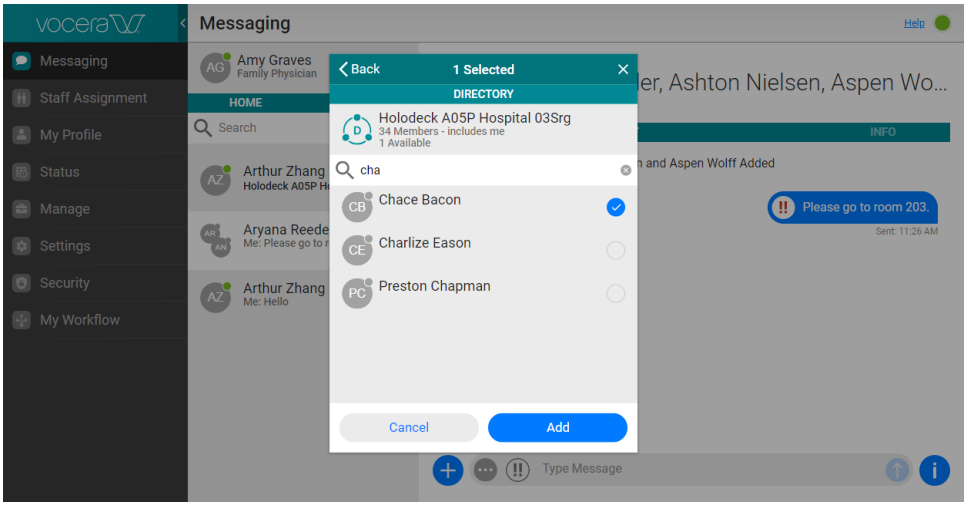
2. Links to your groups and your favorites appear. Do one of the following:
   a. Click a group name to display the members of the group, and then click the icon next to a member to add him or her to the group chat.



b. Click the icon next to a favorite to add this user to the group chat.



c. In the Search box, type two or more characters. From the list of users that match your search text, click the icon next to the user that you want to add to the group chat.

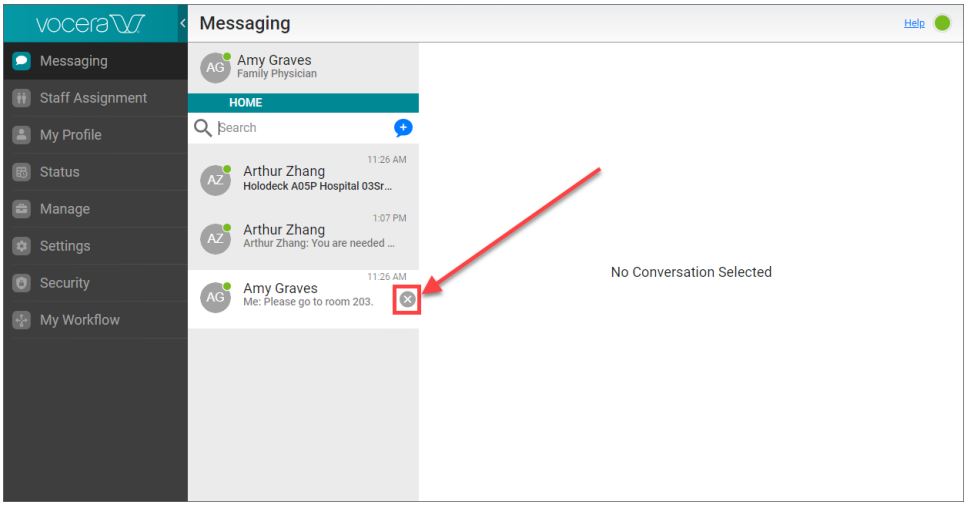


3. Click **Add** to add the new users to the existing group chat. If you are currently in a 1-on-1 conversation, a new group chat is created that contains the users in the conversation and the new users that you have just added.

Leaving a Conversation

You can leave a conversation that you are participating in.

1. To leave a conversation, hover over it and click the X button that appears.



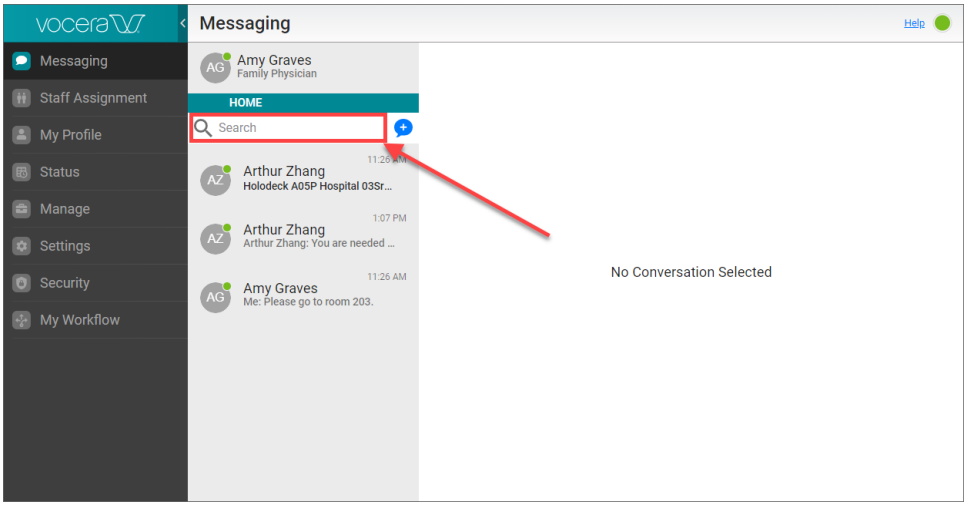
The conversation is moved to the archive, and is no longer displayed in your list of conversations.

Note: You can search archived conversations for specific text or participant names. See Searching Conversations on page 36 for details.

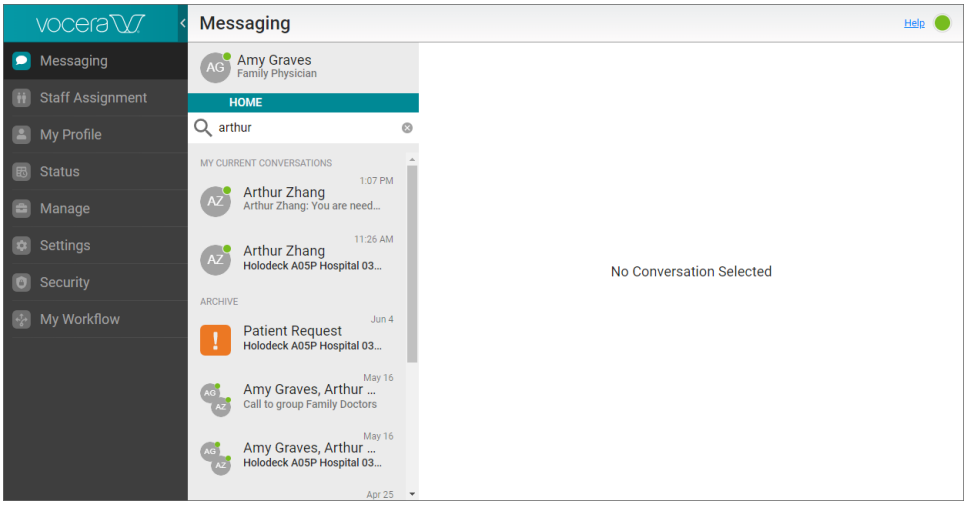
Searching Conversations

You can search for all conversations that contain specific text or include a specific participant. This search can include archived conversations that you have left.

1. In the search field, type the text that you want to match.



A list of matched conversations appears. Conversations that have been archived are grouped separately.



2. Click on a conversation to view it.

About Templates

Your administrator may have created message templates for you to use. These templates enable you to send emergency messages or other messages quickly, as many of the fields in the message have already been defined for you.

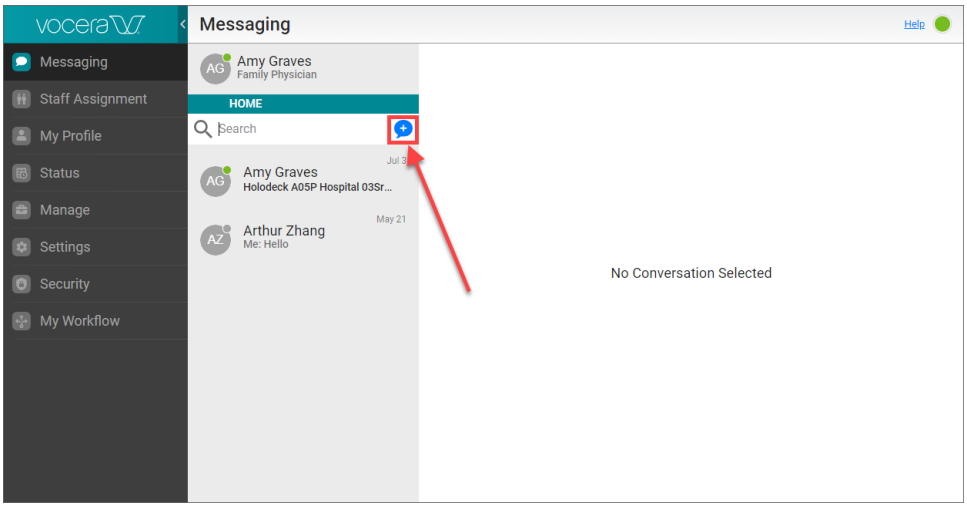
The following types of templates may be available to you:

- Mass Notifications: these are messages that are sent globally or to a group. This template type can be used for emergencies, such as a lockdown. You can specify the level of urgency of the mass notification.
- Staff Events: this is another type of message that can be sent globally or to a group, but is typically used for non-urgent communication. It can have most of its fields pre-populated to make it easier to communicate with a large number of users.
- Patient Events: this is a patient-specific template that can be used to communicate important information about a change in a patient's status, such as a request for transport for patient discharge. You do not need to type the patient details or location to use this type of template.
- Location Events: this is a template that is related to a specific location. This is useful, for example, if you want a room to be cleaned for use by a new patient: you can send a pre-populated message to environmental services, specifying the room number.

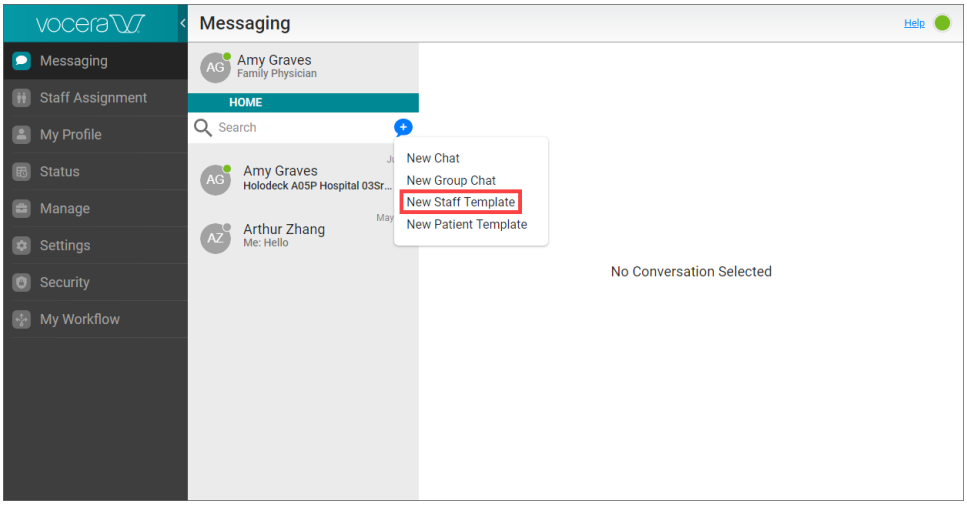
Using a Staff Template

You can use a template to quickly send a mass notification, alert, or other message to other staff members.

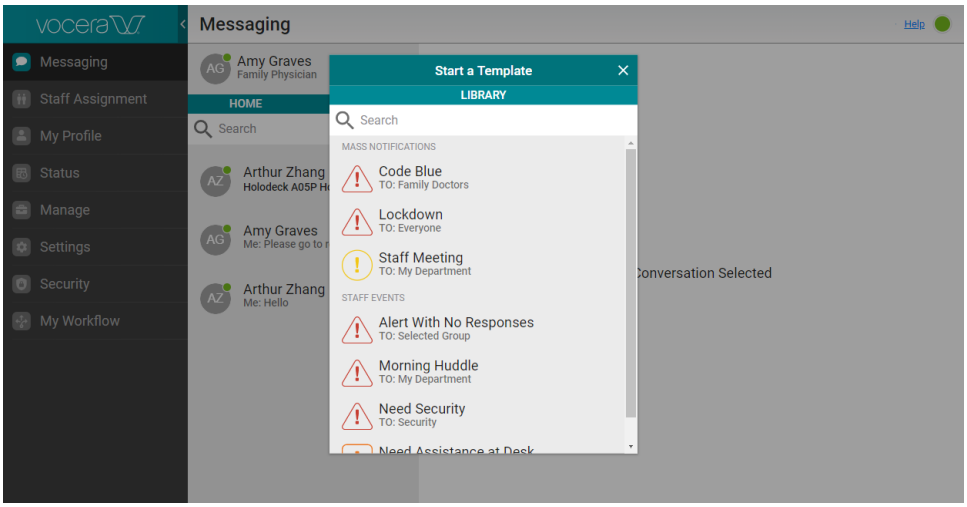
1. In the panel that displays the list of conversations, click the **New** icon.



2. From the pop-up menu that appears, select **New Staff Template**.



The Start A Template panel appears.



In this panel, Mass Notifications templates and Staff Events templates appear if your administrator has made them available to you.

Each template that is available to you displays a **TO:** field that lists the group that will receive the message generated from this template. If **Select A Group** is listed instead of a group name, you will specify the group that is to receive this message when you select this template.

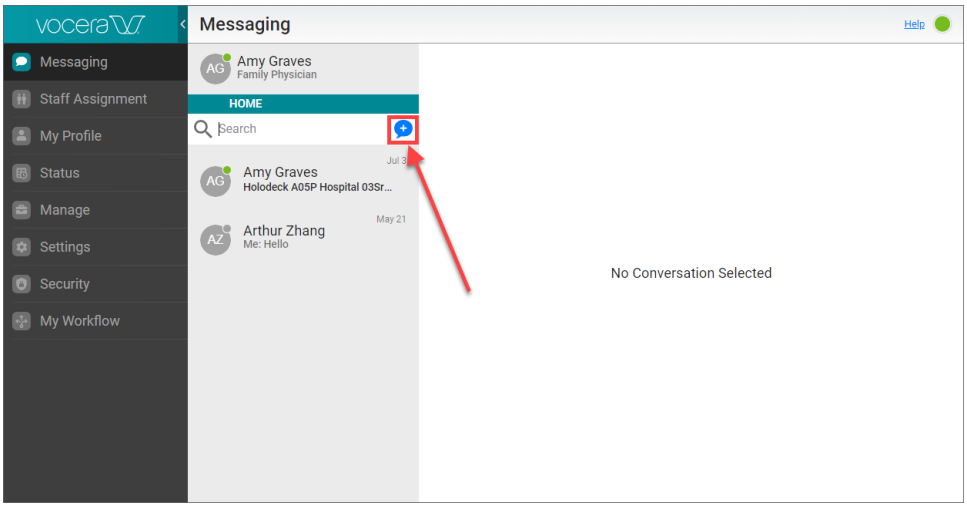
3. In the list of templates available to you, click the template that you want to use.
4. If **Select A Group** is listed in the **TO:** field for the template, select the group that is to receive the message generated from this template.
5. If the template includes fields to be filled in (for example, the time and location of a staff meeting), in the screen that appears, fill in the fields to complete the template.
6. If the template contains message text that can be edited, click in the text field. Type the new text that you want to include.
7. Click **Send** to send the message or alert that you have built from the template.

Using a Patient Template

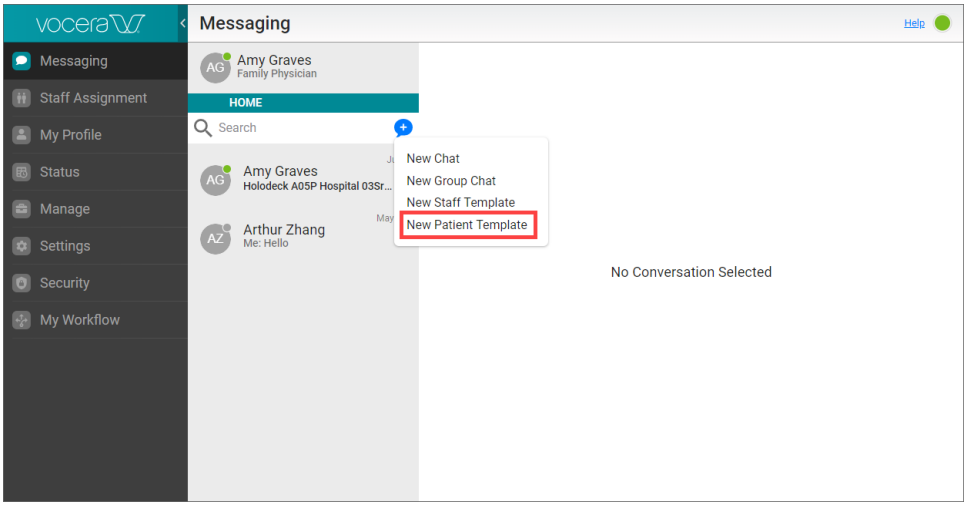
You can use a template to quickly send a mass notification, alert, or other message that is related to a patient.

You can either create a new conversation and select the patient to associate with the patient template, or use a patient template with an existing conversation for which a patient context has been defined.

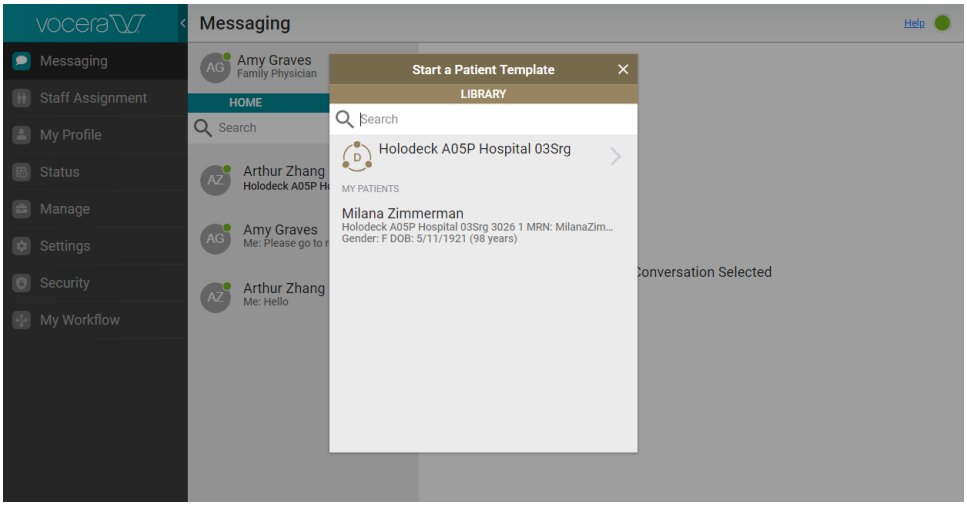
1. If you are creating a new conversation:
   a. In the panel that displays the list of conversations, click the **New** icon.



   b. From the pop-up menu that appears, select **New Patient Template**.

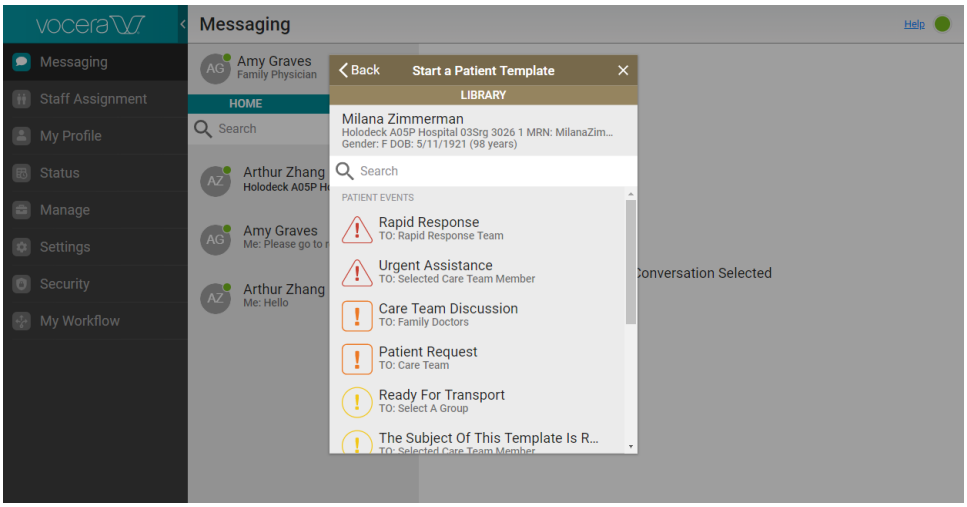


   The Start A Patient Template panel appears.



Note: If patients are not available on your system, you may see the **New Location Template** option instead. In this case, the behavior is the same, but you select a location instead of a patient.

c. Select a patient or location from the list, or select a group and then select a patient or location. A list of available templates appears.



In this panel, Patient Events templates and Location Events templates appear if your administrator has made them available to you.

Each template that is available to you displays a **TO:** field that lists the group that will receive the message generated from this template. If **Select A Group** is listed instead of a group name, you will specify the group that is to receive this message when you select this template.

2. If you are using a template with an existing conversation, click the Add link at the bottom left and select **New Template**.
3. In the list of templates available to you, click the template that you want to use.
4. If **Select A Group** is listed in the **TO:** field for the template, select the group that is to receive the message generated from this template. If the template sends a message to a specific team member, select the team member.
5. If the template includes fields to be filled in (for example, the time and location of a staff meeting), in the screen that appears, fill in the fields to complete the template.
6. If the template contains message text that can be edited, click in the text field:

   The text disappears. Type the new text that you want to include.

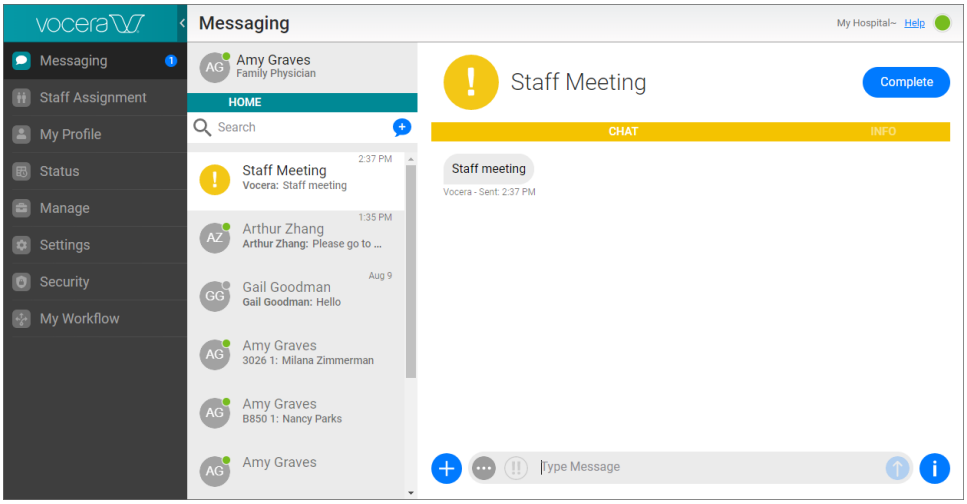
   Type the new text that you want to include.
7. Click **Send** to send the message or alert that you have built from the template.

Completing a Template Message

If you have sent a message using a template, you can mark it as complete as soon as you are satisfied that the message has been received.

To complete a template message, click on the Complete button:

1. Click **Complete**.



2. Click **OK** to confirm that you want to complete the message.

The message is removed from your list of conversations. This conversation is still available in the conversation archive.

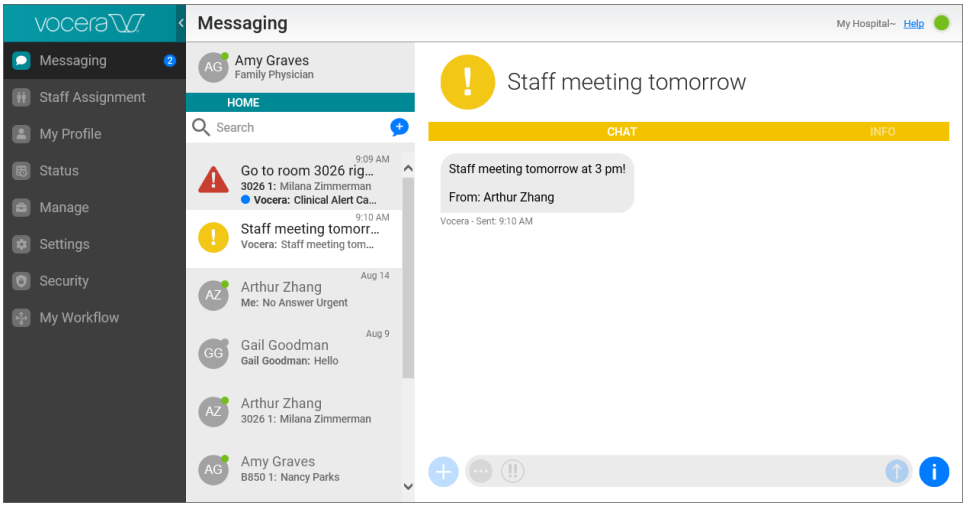
About Personal Messages

An administrator can send you a personal message if he or she needs to communicate with you.

This message appears in your list of conversations. Click on the conversation link to view it.

About Mass Notifications

If your administrator has assigned you to a group, you may receive mass notifications sent to all members of the group.



The icon next to the mass notification indicates the priority:

Icon	Priority
	High
	Medium
	Low

About Favorites

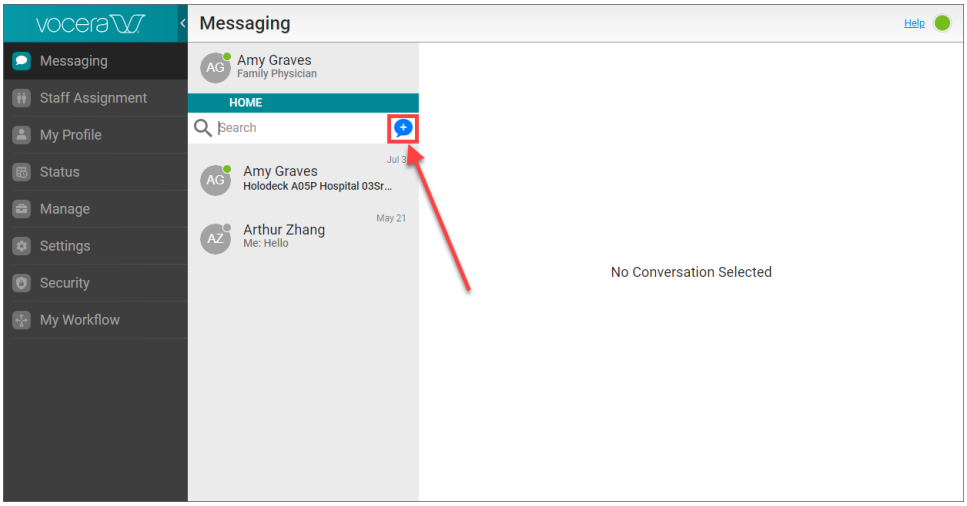
The Favorites feature lets you create a list of users and groups you communicate with frequently.

Maintaining a favorites list allows you to find a user or group without having to search the directory. Favorites can be individuals or groups.

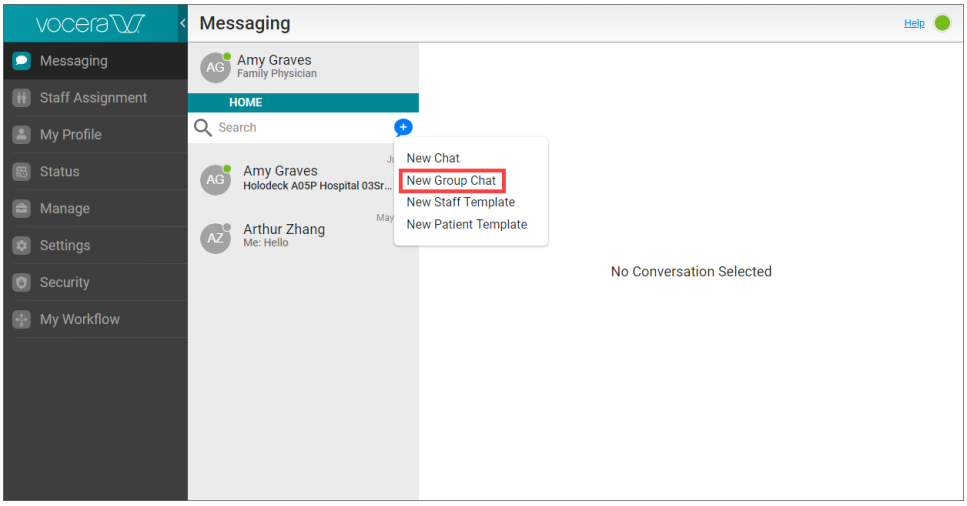
Adding a Favorite

You can use the Start a Group Chat panel to add a favorite to your list. You can also remove a favorite that you have previously specified.

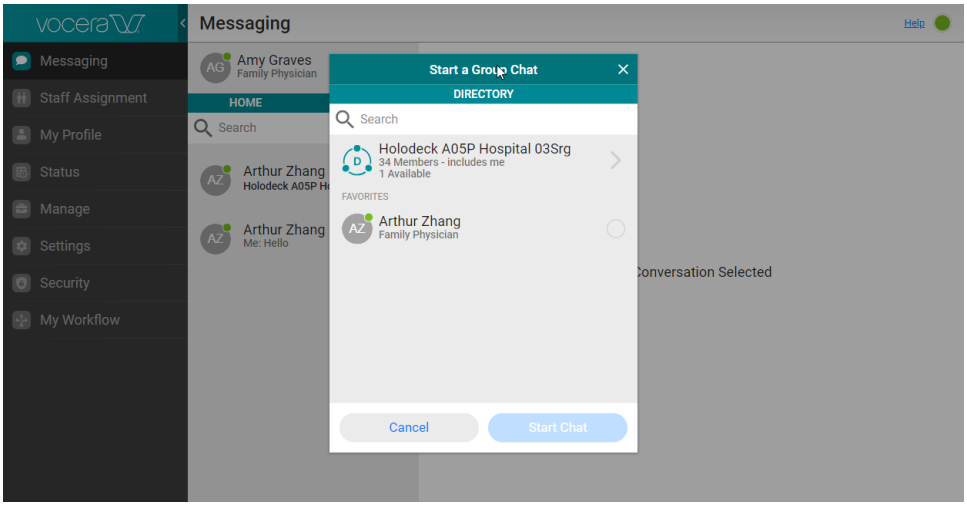
1. In the panel that displays the list of conversations, click the **New** icon.



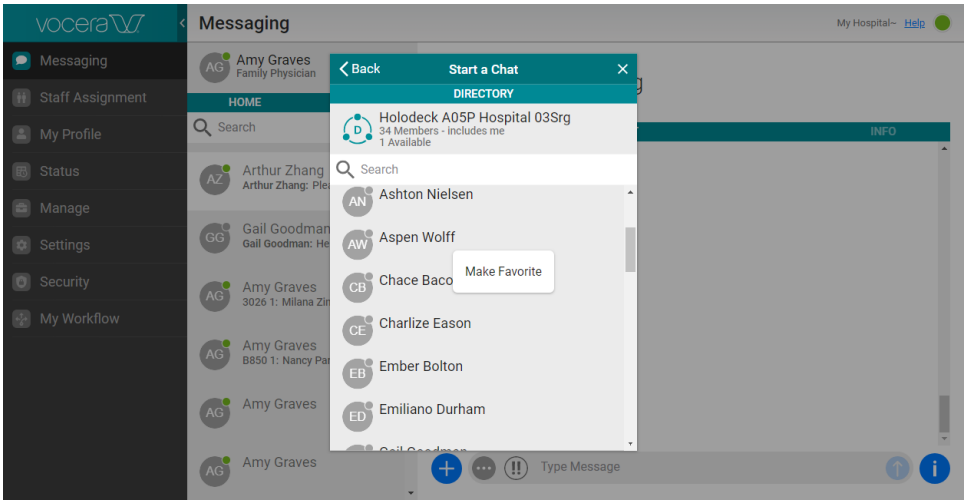
2. From the pop-up menu that appears, select **New Group Chat**.



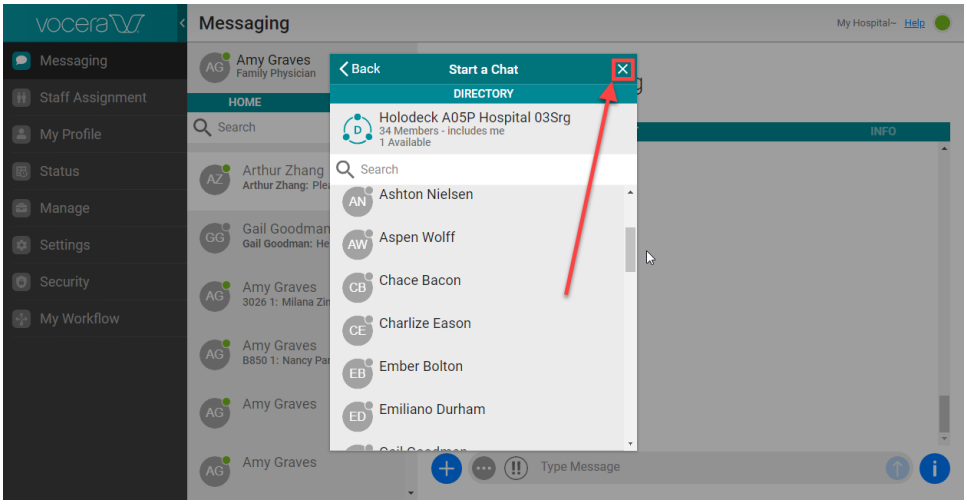
The Start A Group Chat panel appears.



3. Locate the group or user that you want to add as a favorite or remove from your favorites list.
4. Right-click on the group or user, and select **Make Favorite** to add the favorite, or select **Remove Favorite** to remove the favorite.



5. Click the X at the top right to exit, or follow the instructions in Starting a Group Chat on page 25 to start a new group chat.


Messaging
My Hospital~ Help
Messaging
Staff Assignment
My Profile
Status
Manage
Settings
Security
My Workflow
Amy Graves
Family Physician
HOME
Search
Arthur Zhang
Gail Goodman
Amy Graves
Amy Graves
Amy Graves
Back
Start a Chat
DIRECTORY
Holodeck A05P Hospital 03Srg
34 Members - includes me
1 Available
Search
Ashton Nielsen
Aspen Wolff
Chace Bacon
Charlize Eason
Ember Bolton
Emiliano Durham
INFO
Type Message

Personal Titles

If a contact has a personal title defined (such as MD or RN), this title always appears after the user's name.

Staff Assignment

This section provides an overview of the Vocera Platform Staff Assignment module and describes how to set it up for initial use.

- About the Vocera Platform Staff Assignment Guide on page 50
- Configuring Staff Assignment on page 51
- The Staff Assignment Home Page Layout on page 62
- Using Staff Assignment on page 64

About the Vocera Platform Staff Assignment Guide

The Vocera Platform Staff Assignment Guide describes how to perform tasks using the Vocera Platform Staff Assignment application.

You can use this document as you work with Staff Assignment, 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 Staff Assignment console.

Staff Assignment Prerequisites

Before you begin installing Staff Assignment, ensure that you have installed the following adapters, services, and solution packages.

The following table lists all required Vocera Platform components to install Staff Assignment.

Required Adapters Services	Descriptions
Vocera Platform	Version 6.1.0.8 or later.
Vocera XMPP Adapter 4.1.0	The Vocera XMPP Adapter enables XMPP communication between Vocera users using XMPP clients by acting as the XMPP server for its configured domain. For detailed configuration information, refer to the Vocera XMPP Adapter 4.1.0 documentation available on the Vocera Documentation Portal.
Vocera DataUpdate Adapter	The Vocera DataUpdate adapter allows to make changes to data in the system when a Data Update Rule is triggered. A Data Update adapter rule is configured with a set of pairs of attribute paths and values. When the Data Update adapter is enabled and a rule is triggered, the path is evaluated relative to the object that triggered the rule.
Staff Assignment Client	TheStaff Assignment client component for Vocera Platform
Staff Assignment Service	The Staff Assignment server component for Vocera Platform
Vocera Assignment Group Sync Adapter 2.0.0	The Vocera Assignment Group Sync Adapter is used to map assignments to groups, and vice-versa. This facilitates the transformation of assignments received from an external assignment system, to groups which can be utilized by the Vocera Voice Server. For detailed configuration information, refer to the Vocera Assignment Group Sync Adapter documentation available on the Vocera Documentation Portal.

ENGAGE 2.1	• ENGAGE 2.1 with the following workflows:
	  • Manage Location Workflow
	  • Manage Functional Role Workflow
	  • Staff Assignment History Workflow

Configuring Staff Assignment

Configure Staff Assignment in the Vocera Platform Web Console to allow users to access and use the Staff Assignment application.

To configure Staff Assignment, you must review and install the required perquisites described in theStaff Assignment Prerequisites on page 50 section, and perform the following configuration tasks:

- Create a Staff Assignment facility
- Import beds, rooms, and departments
- Create single or multiple-bed locations
- Create functional roles
- Assign and link groups to single or multi-bed locations
- Assign department level permissions.

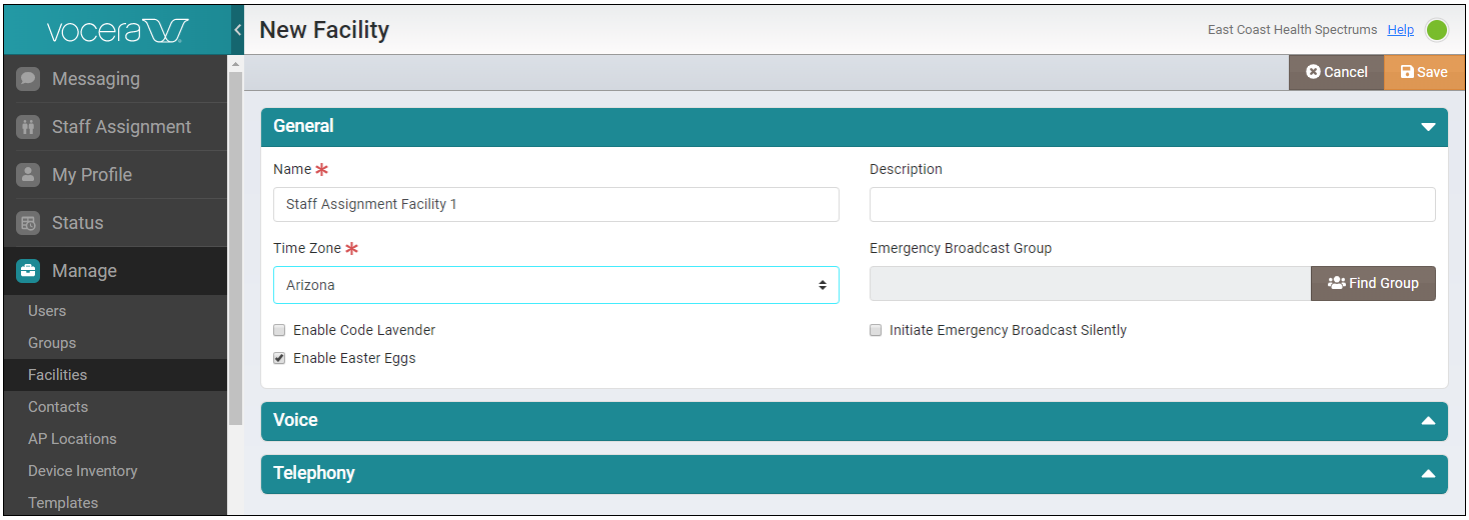
Creating a Staff Assignment Facility

Manually create a facility in the Web Console to set up Staff Assignment.

You can also import your facilities for Staff Assignment using the **Bulk Actions** import function available in the Web Console

The following task describes the process to create a single facility inWeb Console for configuringStaff Assignment:

1. Select **Facilities** in the **Manage** section of the navigation bar.
   The Hospital Locations page displays.
2. Click the **Add Facility** button on the top right hand corner.
   The New Facility page displays.
3. In the General section, specify a value for the **Name** and **Time Zone** configuration fields.
   For example, the following screenshot shows a facility named “Staff Assignment Facility 1” and “Arizona” time zone value selected for the Time Zone field.



For detailed information on other configuration fields in the New Facility page, see Adding a Facility on page 186.

4. Click **Save** to save the new facility information to your system.

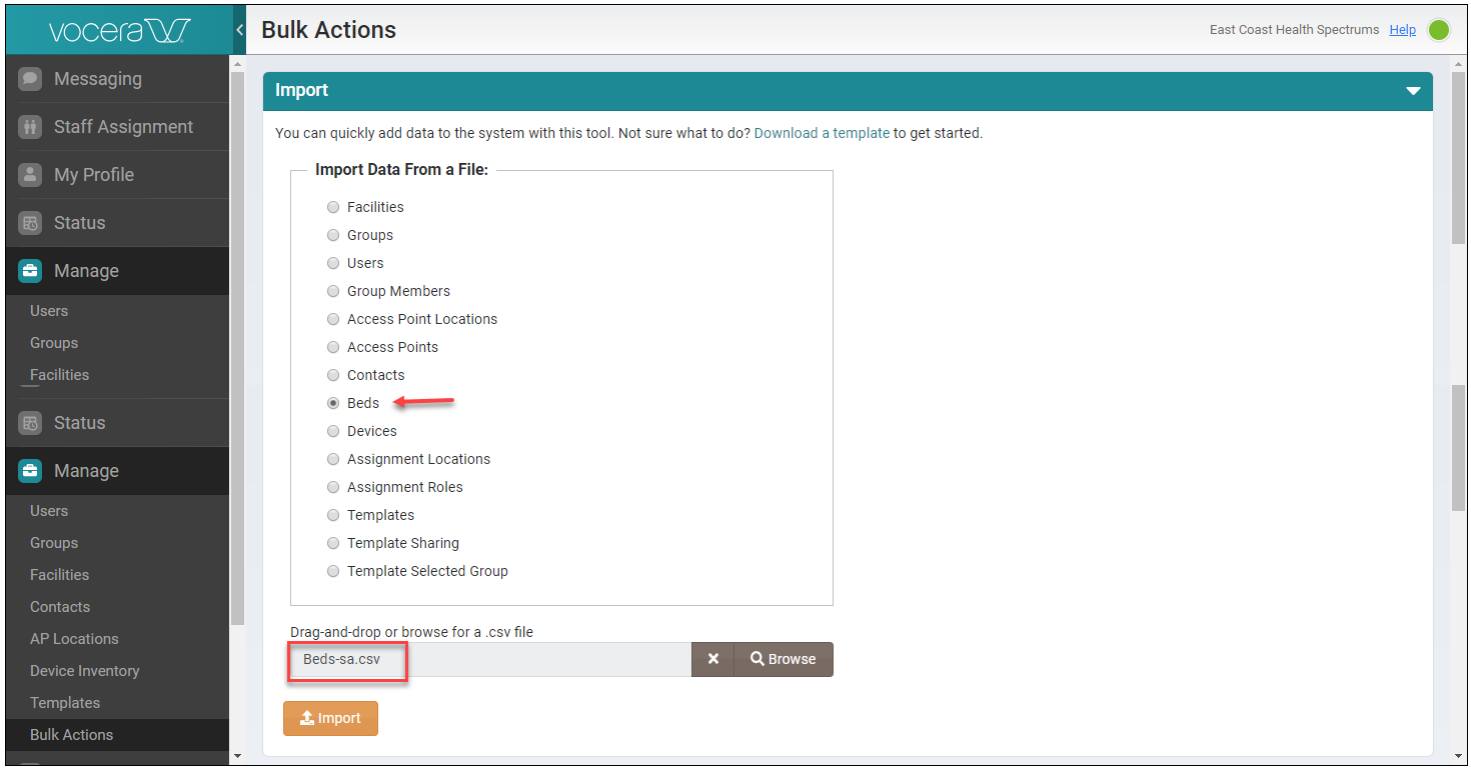
Importing Beds, Rooms, and Departments

Import data related to beds, rooms, and departments (unit) to Vocera system.

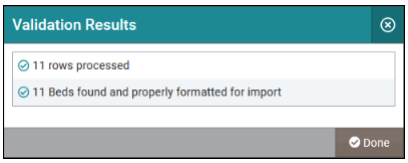
Before you import Beds, Rooms, and Units (departments) data, you must enable the data update rules. For information on enabling data update rules for beds, see Enabling Matching Rules for Import on page 54.

Note: The imported CSV file displays a Unit column that represents Departments that you are importing.

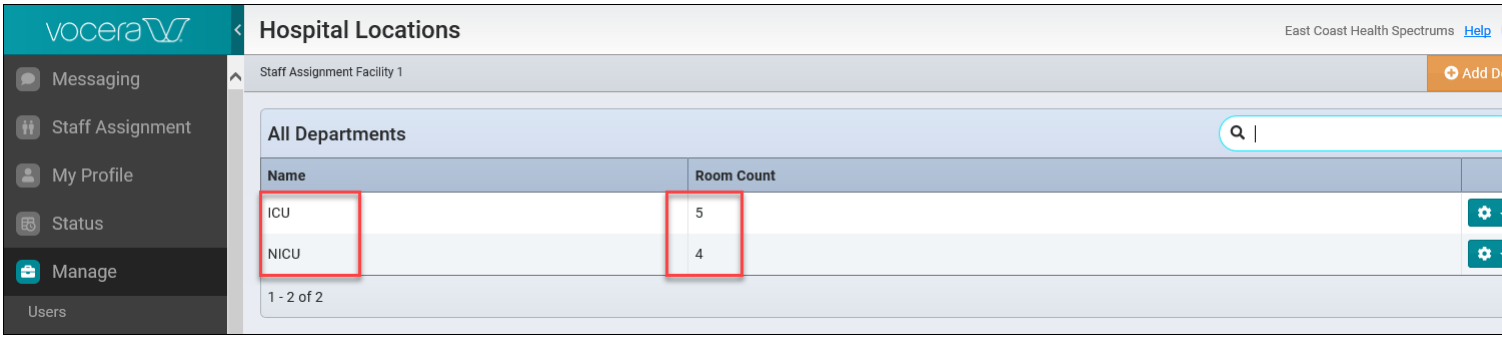
1. Navigate to **Bulk Imports** in the navigation bar and select the **Beds** radio button in the **Import** section.
2. Click the **Browse** button to browse your computer and upload or drag-and-drop your `Beds.CSV` file.



System validates the imported CSV file contents and displays Validation Results with information on the data processed. For example, for the `Beds-sa.CSV` file, the system might display the number of rows processed and the information on Beds formatted properly for the import action.



3. Click **Done** to exit out of the Validation Results dialog box.
4. Navigate back to **Facilities** and click on the facility that you created for Staff Assignment in Step 2.
   The staff assignment facility page displays with departments and room information associated with this facility.
   For example, the following screenshot displays the department names and number of rooms imported and automatically updated to the “Staff Assignment Facility 1”.

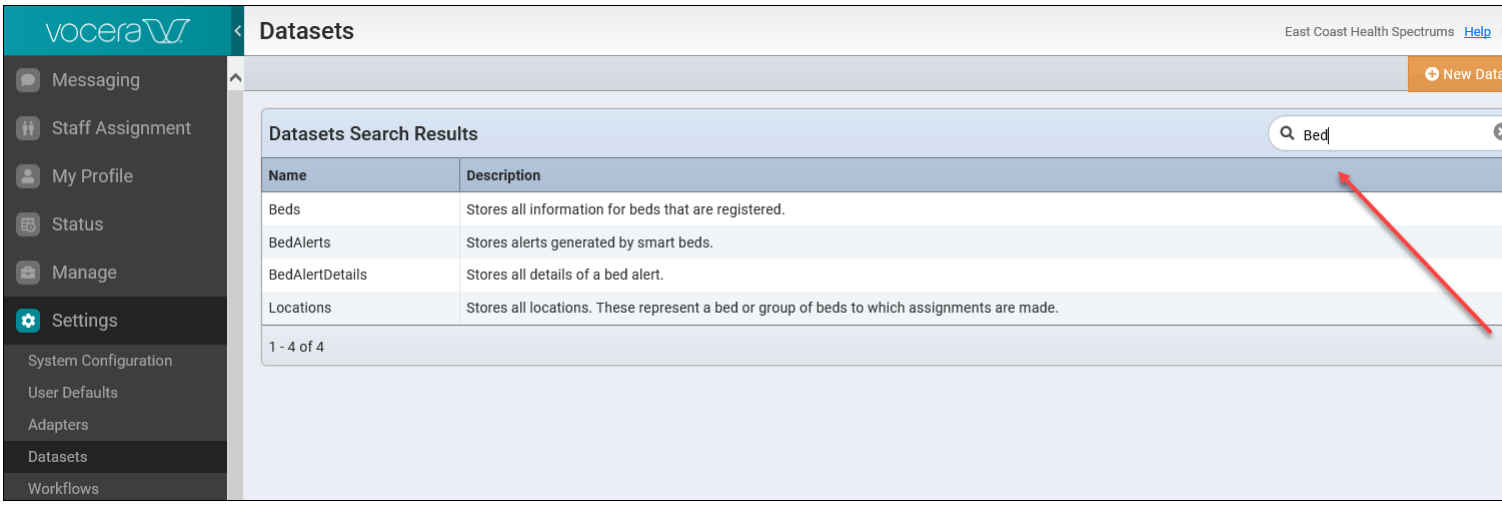


You can also click on each department for this facility and view the rooms and bed count associated with the department.

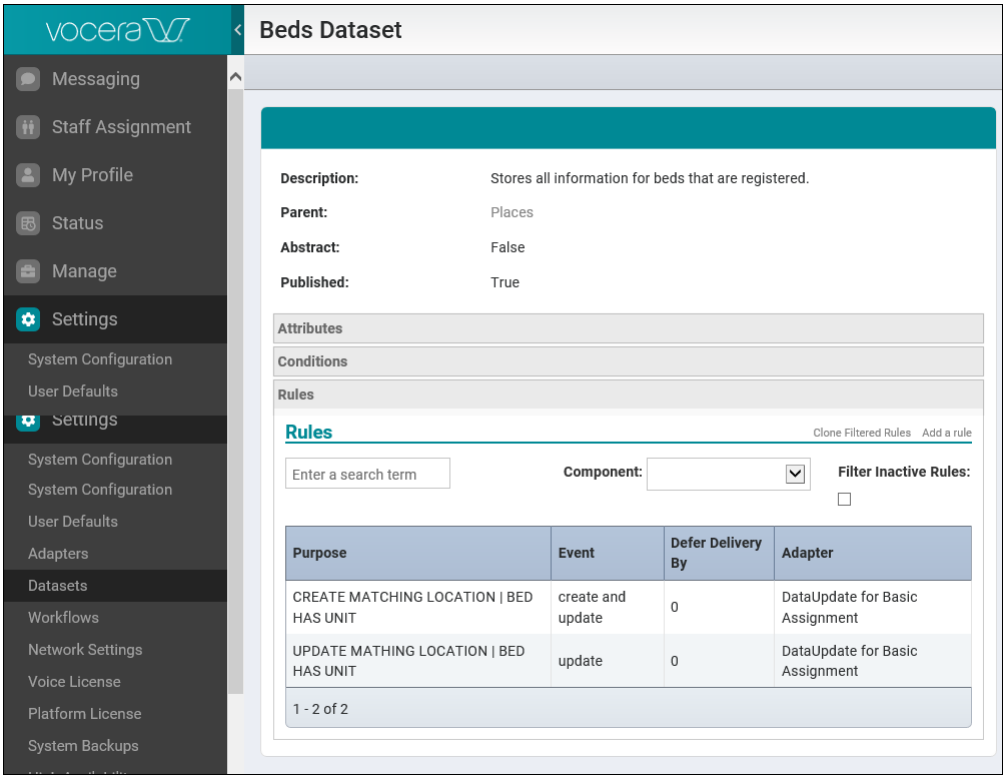
Enabling Matching Rules for Import

Enable dataset rules to import units (department), beds, and rooms.

1. Navigate to the **Settings** section in the navigation bar and select **Datasets**
   The Datasets page displays with a list of all available datasets in the system.
2. Enter "Beds" in the search bar on the top left corner and Press the **Enter** key.
   The system displays a list of datasets with the word "Beds"



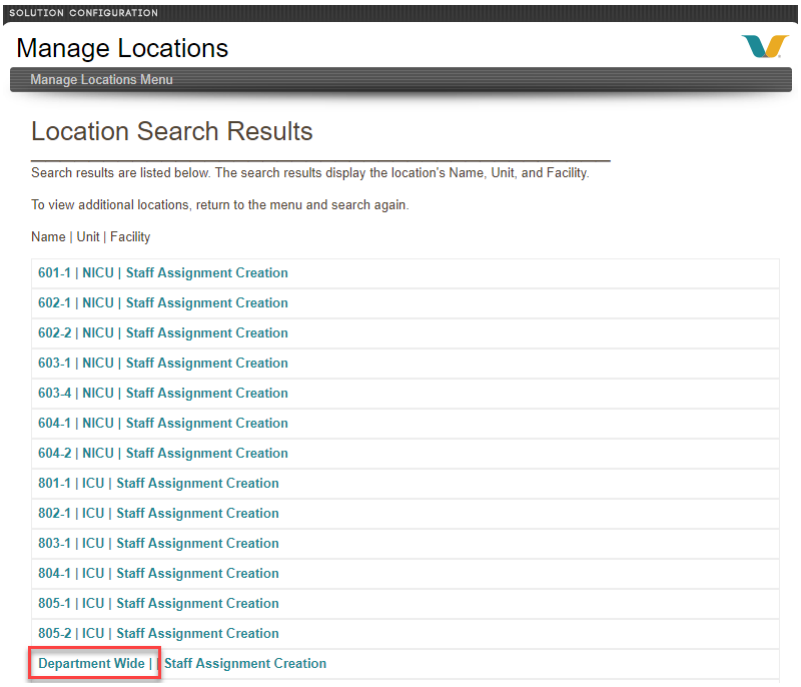
3. Click on Beds dataset to view the details.



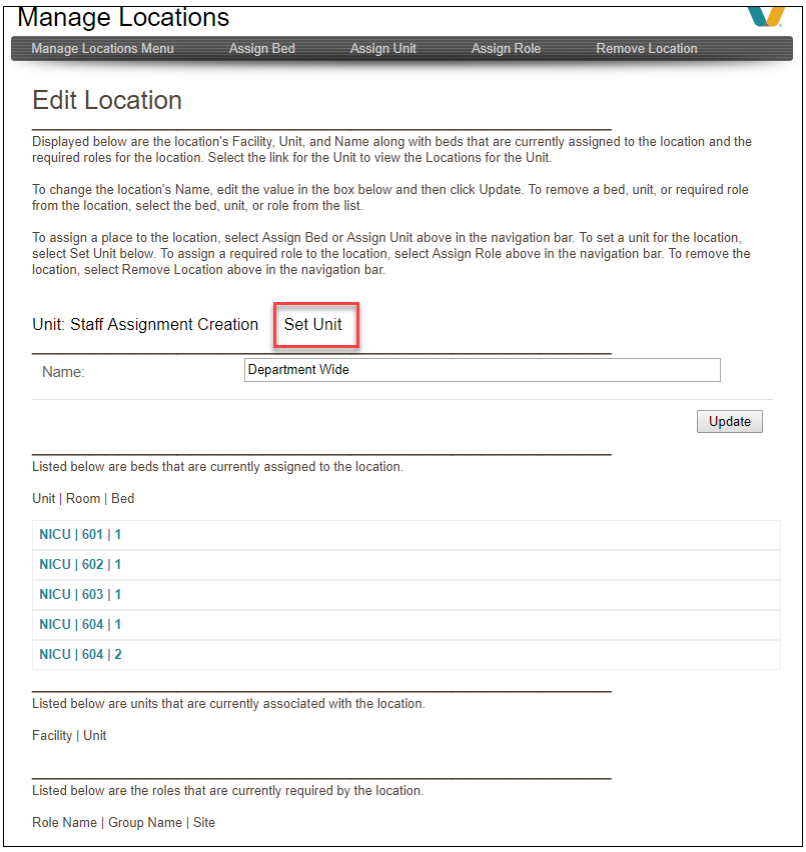
Creating Locations

Depending on your Staff Assignment requirements you can create single or multiple bed locations.

1. To create single bed locations, enable the Beds dataset rules as described in Enabling Matching Rules for Import on page 54.
2. To create multiple bed locations, follow these steps:
   a. Import your `AssignmentLocations.CSV` file to the system using the **Import** function from **Bulk Actions** in the **Manage** section of the navigation bar.
   b. Click **My Workflow** in the navigation bar and select **Manage Locations**
   The Manage Locations page displays.
   c. Enter your staff assignment facility name in the Facility field and click **Search**
   The Location Search Result displays a list of Name, Unit (Department), and Facility for the Facility name that you entered in the search field.
   For example, the following screenshot displays a list of Name (Room), Unit (Department), and Facility information for Staff Assignment.



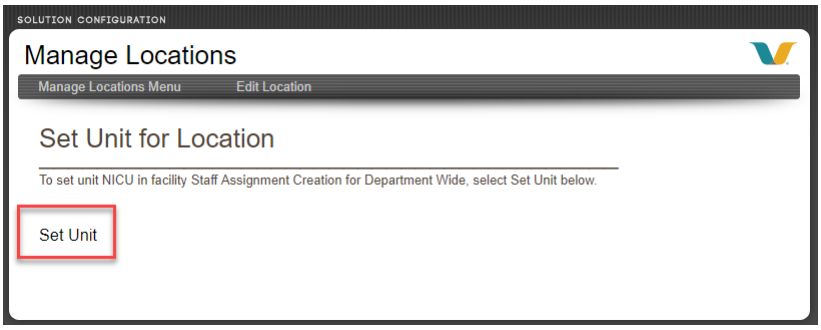
   d. Click **Department Wide** to edit the location information.
   The Edit Location page displays
   e. Click on **Set Unit** to select the unit that you want to set for this location.



Note: You must follow these steps for each multiple bed location that you created.

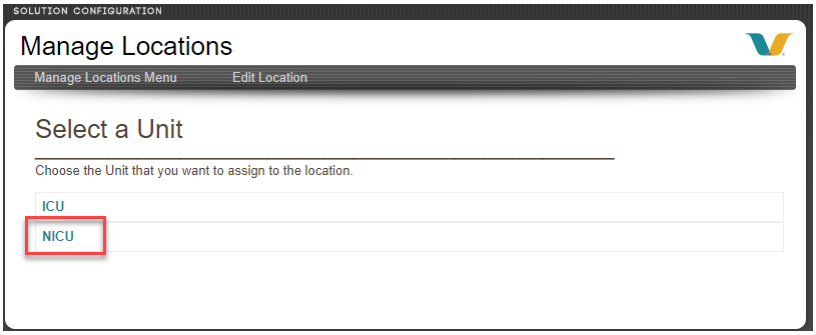
The Set Unit for Location page displays.

f. Click **Set Unit** in the Set Unit for Location page.

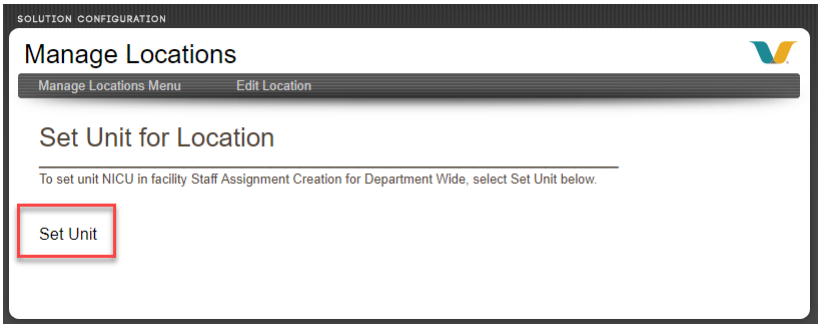


g. Choose a Unit that you want to assign to this location.

For example, in the following screenshot there are two units; ICU and NICU and we selected NICU to unit to be assigned to this location.



h. Click **Set Unit** in the set NICU as the unit for this location..

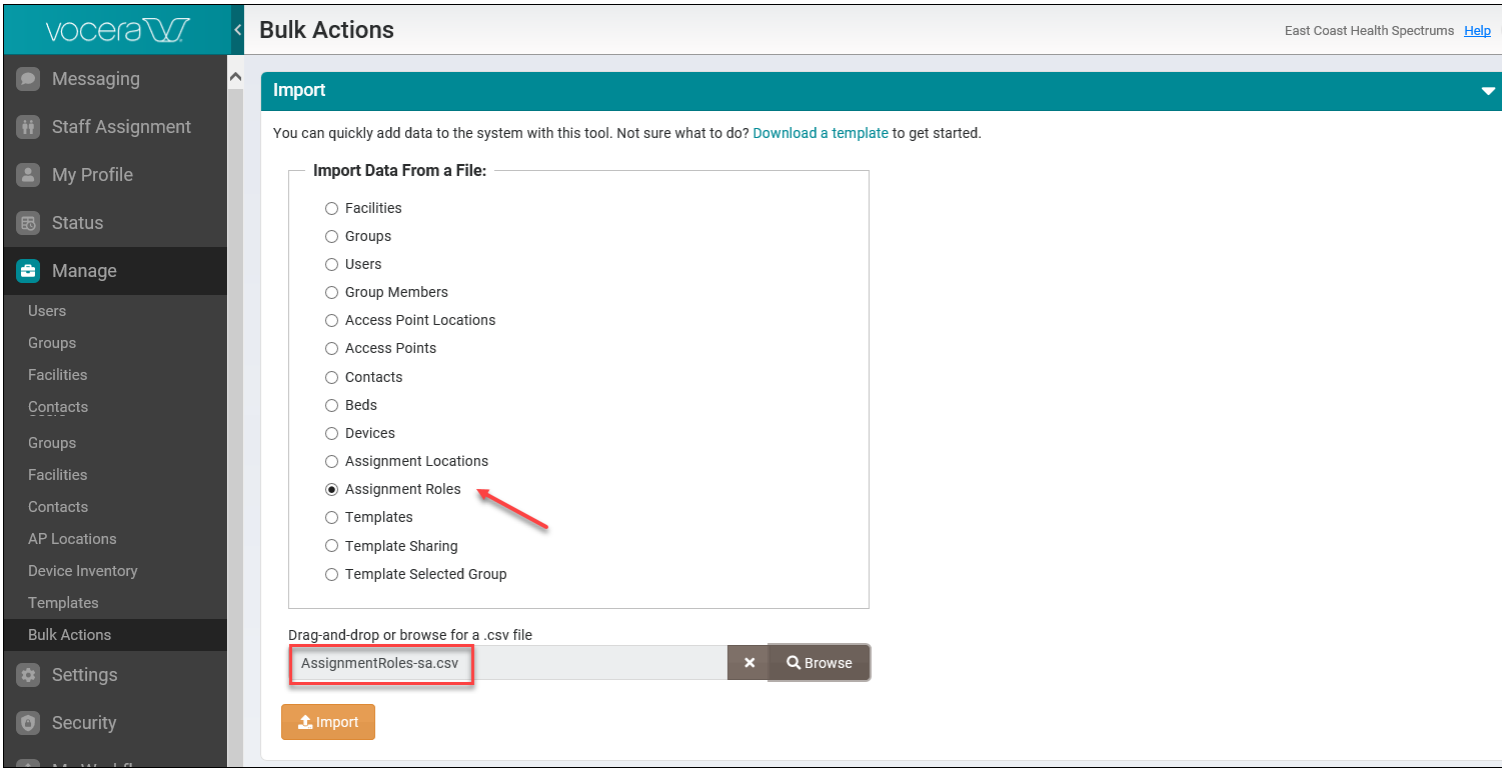


Creating Functional Roles

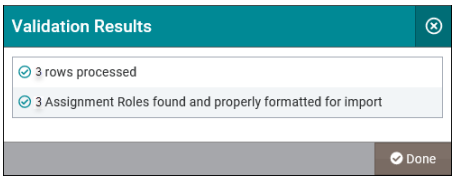
Create functional roles using the Import function in **Bulk Actions** in the **Manage** section of the navigation bar.

Before you begin, verify that you have an `AssignmentRoles.CSV` file functional roles data that you can upload for creating multiple functional roles. For information on `AssignmentRoles.CSV` file and **Bulk Actions**, see Importing Data to the System on page 255.

1. Navigate to **Bulk Imports** in the navigation bar and select the **Assignment Roles** radio button under the **Import** section.
2. Click the **Browse** button to browse your computer and upload or drag-and-drop your `AssignmentRoles.CSV` file.



System validates the imported CSV file contents and displays Validation Results with information on the data processed. For example, for the `AssignmentRoles-sa.CSV` file, the system might display the number of rows processed and the information on Beds formatted properly for the import action.



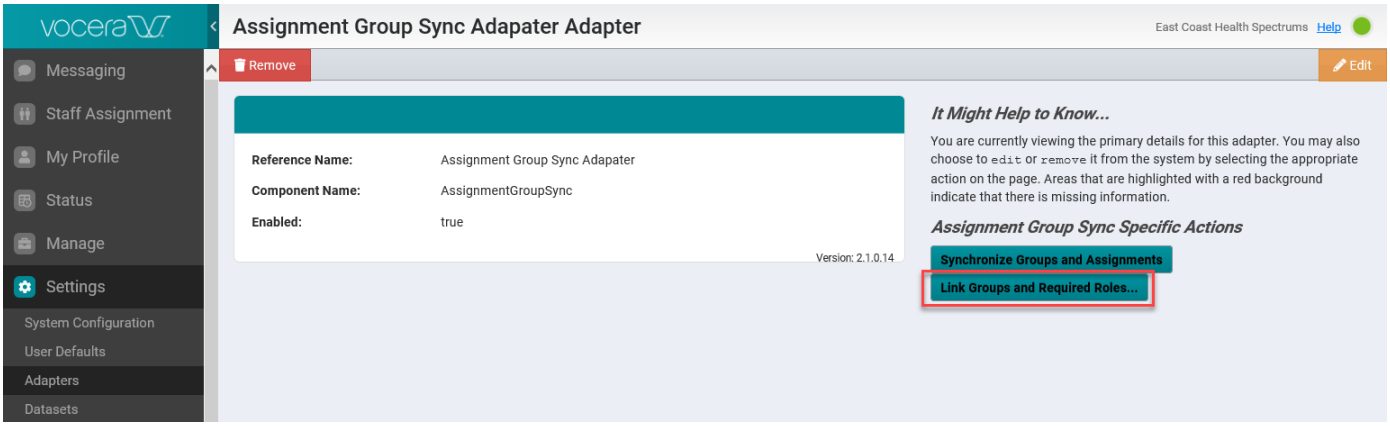
3. Click **Done** to exit out of the Validation Results dialog box.

Assigning Roles and Linking Groups

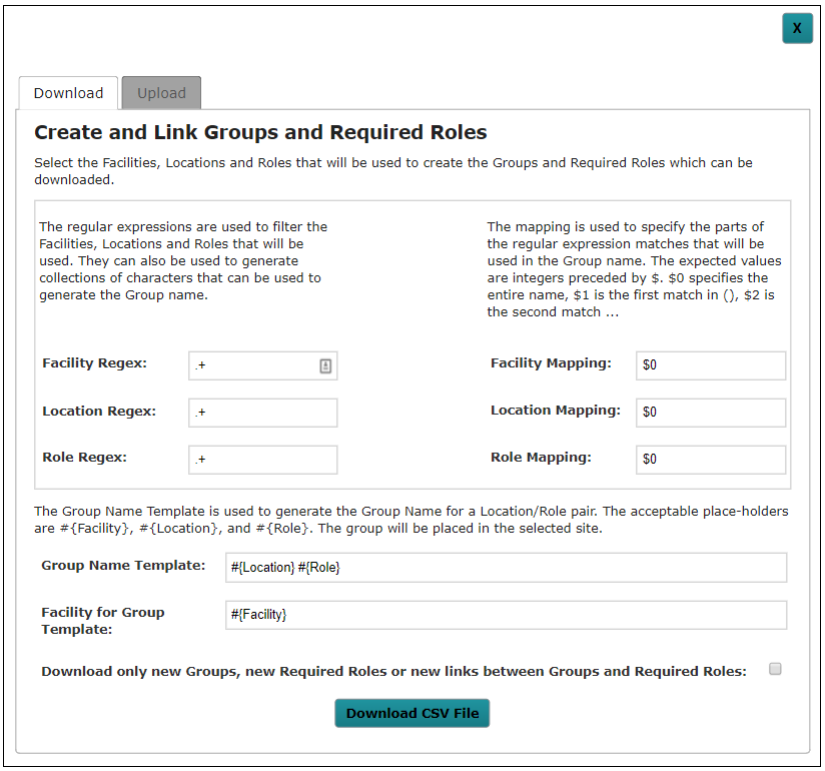
Assign functional roles and create groups to synchronize your single or multiple bed locations, functional roles, and assignments with the help of the Assignment Group Sync adapter in the Vocera Platform Web Console.

1. Navigate to **Adapters** in the **Settings** section of the navigation bar in the
2. Locate the **AssignmentGroupSync** adapter and click on the adapter to display the AssignementGroupSync Adapter page

   The AssignementGroupSync Adapter page displays.
3. Click on **Link Groups and Required Rules** on the bottom right hand side of the adapter page to export the `.CSV` file so that you can re-import this file after verification.



The Create and Link Groups and Required Roles dialog box appears.



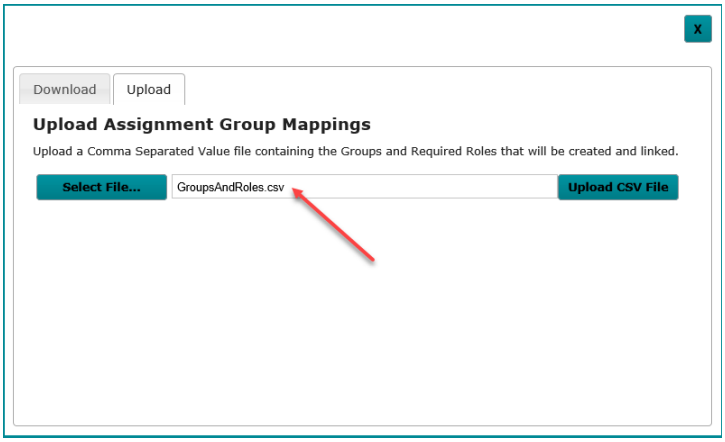
4. In the Create and Link Groups and Required Roles dialog box enter a value for the following fields:
   - Specify the facility, location, and functional role regular expressions (regex) that will be used to identify the locations and functional roles.
   - Specify the mapping values associated with the Facility, Location, and Role regular expressions fields to be used in the Group name.
   - Specify the values for The Group Name Template. This field is used to generate the Group Name for a Location/Role pair. The acceptable place-holders are #{Facility}, #{Location}, and #{Role}. The group will be placed in the selected facility.
   - Select the checkbox at the bottom of the dialog box to filter the rows where the groups and required role already exist and are linked.

   For more information, refer to Linking Groups and Required Roles section in the Vocera Assignment Group Sync Adapter documentation.
5. Click **Download CSV File** to download the `GroupsandRoles.CSV` files to your computer.
6. Open the downloaded `GroupsandRoles.CSV` file and validate the information in this file.

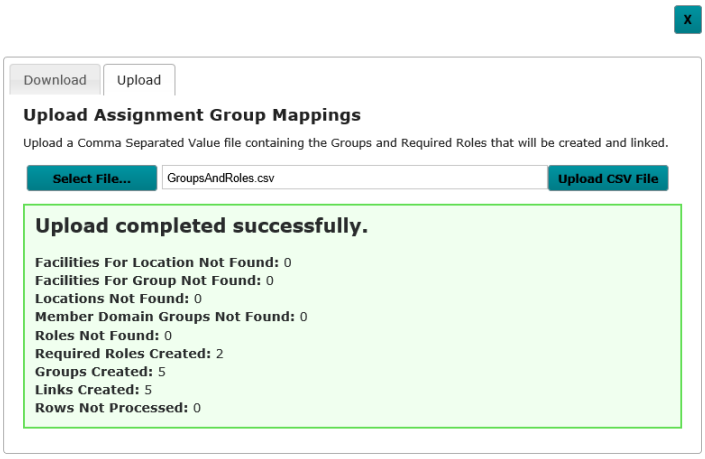
Note:

- The **Remove Users on Logout** column in the `GroupsandRoles.CSV` can be set to "True" if you wish to remove a group member on logout.
- The **Member Domain Group** and **Facility for Member Domain Group** can be filled in to allow users within the group to Add or Remove themselves from groups.

7. Click **Upload** tab to display the Upload Assignment Group Mappings dialog box.
8. Click **Select File** to select and upload the validated `GroupsandRoles.CSV` file from your computer.
   The following screenshot displays the `GroupsAndRoles.CSV` file uploaded to the system.



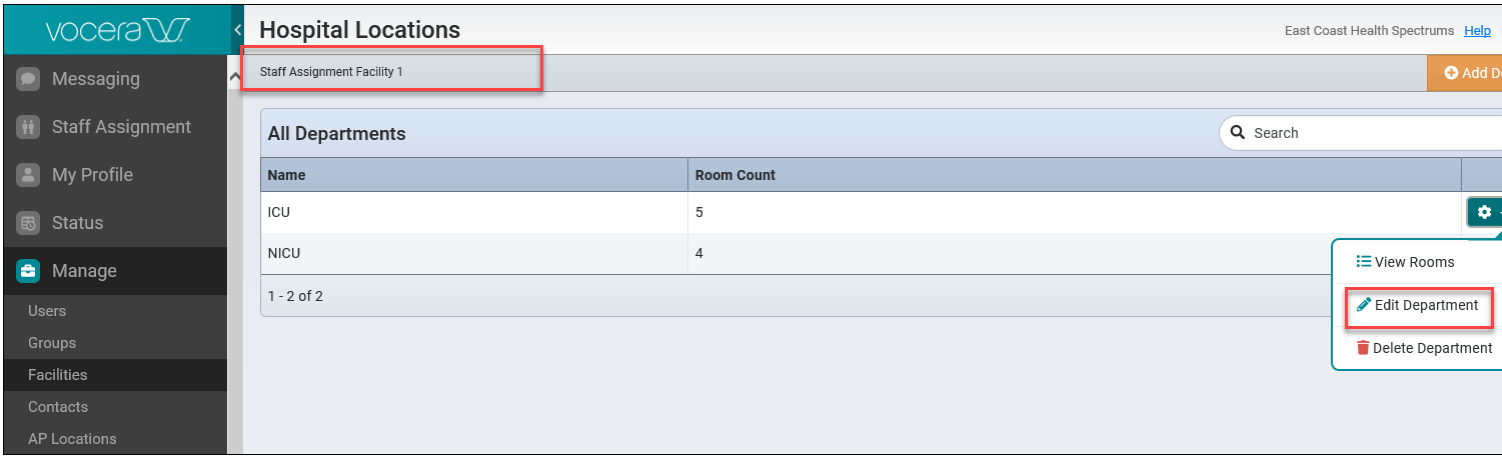
9. Click **Upload CSV File** to upload the `GroupsandRoles.CSV` to the system.
   A success message displays to confirm that the upload process is completed. For example, the following screenshot shows a success message that displayed after uploading the `GroupsandRoles.CSV` file.



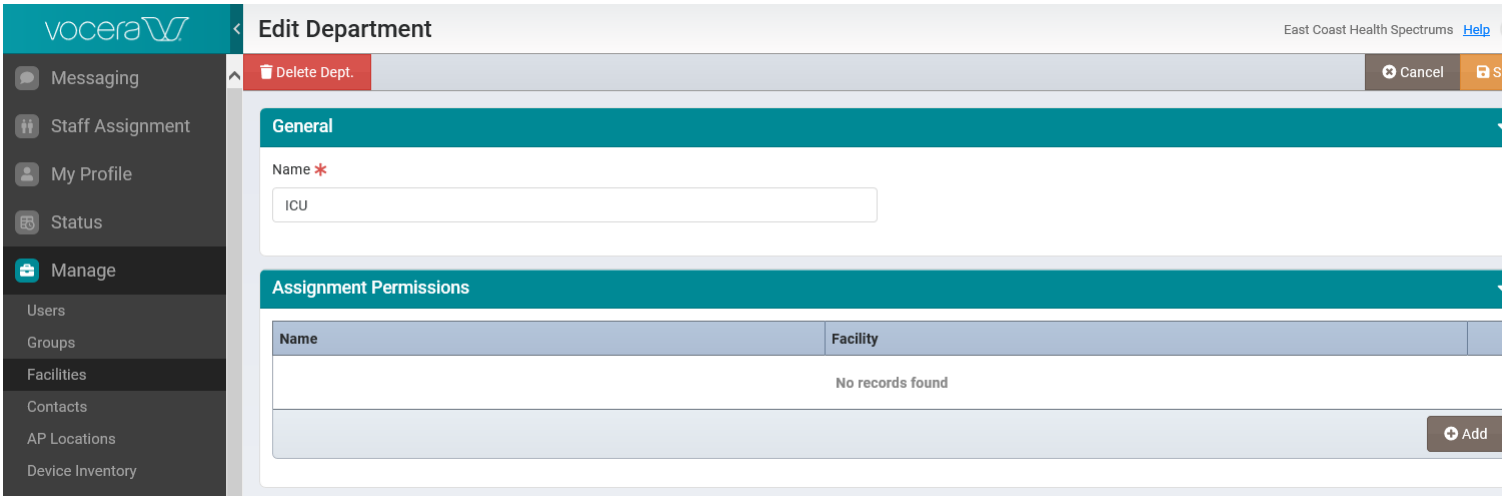
Assigning Department Level Permissions

Assign permissions at department level to manage Staff Assignment.

1. Select **Facilities** in the **Manage** section of the navigation bar to locate your Staff Assignment facility.
2. Click on your Staff Assignment facility to display all departments within this facility.
3. Select **Edit Department** in the drop down menu.



The Edit Department page displays.

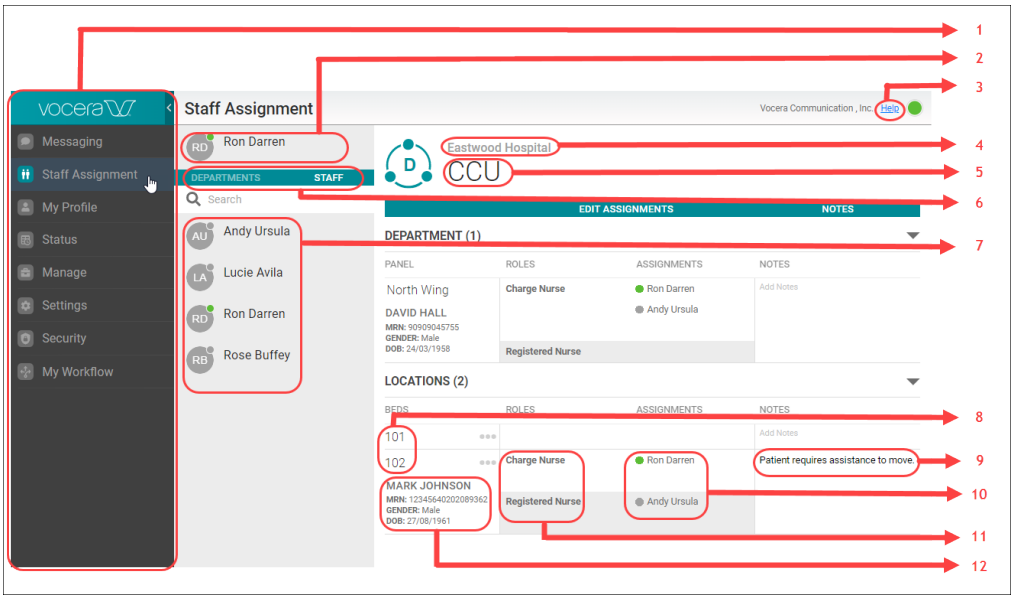


4. In the Assignment Permissions section, click **Add** to display the Find a Group dialog box.
   Use the Find a Group dialog to:
   - Enter the group name in the **Group Name** field to search for a group in system.
   - Select multiple groups from the list.
   - Toggle the **Facility Name** field to view all facilities available in your system and refine your search.
5. In the **Group Name** field, enter the name of the group that you want to allow to make assignments within the department.
   You can also select more than one group names from the Find a Group dialog box and click to allow multiple groups to make assignments within the department.
6. Click **Select Groups** to close the Find a Group dialog.
7. Select one of the following to close the Edit Department page:
   - **Save**— to save the edited department in the system.
   - **Cancel**— to return back to the All departments page without changing the department name.

The Staff Assignment Home Page Layout

This topic describes the layout and the user interface controls available in the Staff Assignment module.

The following figure shows the basic user interface controls in the Staff Assignment module:



The following table describes the basic user interface controls in the Staff Assignment module:

Number	Description
1	This is the Navigation Panel. It provides quick access to the various areas within Vocera Platform. As new modules are made available within the Vocera Platform, the navigation panel expands to include those modules too.
2	Displays the name of the logged in user.
3	Web link to the context-sensitive help.
4	Displays the facility name.
5	Displays the department name.
6	Displays the two main tabs within the Staff Assignment. The tabs are: • Departments—Displays the departments within the selected facility. • Staff—Displays the staff members within the selected department.
7	Displays the names of the assigned staff members within the selected department.
8	Displays the bed number.
9	Displays the notes about a patient. Notes indicate specific information about the patient and are helpful for staff members to take decision accordingly.

Number	Description
10	Displays the names of staff members that are currently assigned to a patient.
11	Displays the roles of staff members that are currently assigned to a patient.
12	Displays the details of the patient such as patient name, MRN number, gender, and date of birth.

Using Staff Assignment

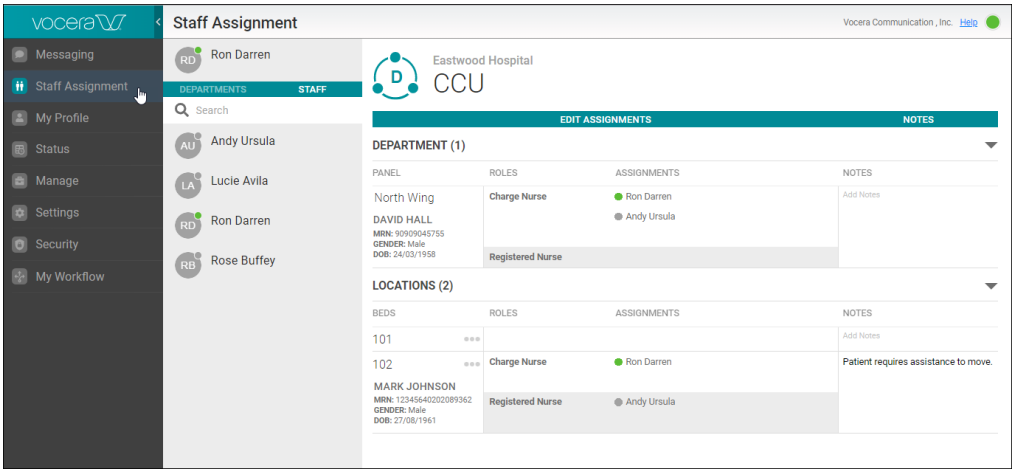
Use the Staff Assignment feature to assign nurses to beds. It allows you to view departments and search for staff members within a department, send messages to care team or individual staff members, remove a staff assignment, and add notes related to a patient.

Viewing Departments

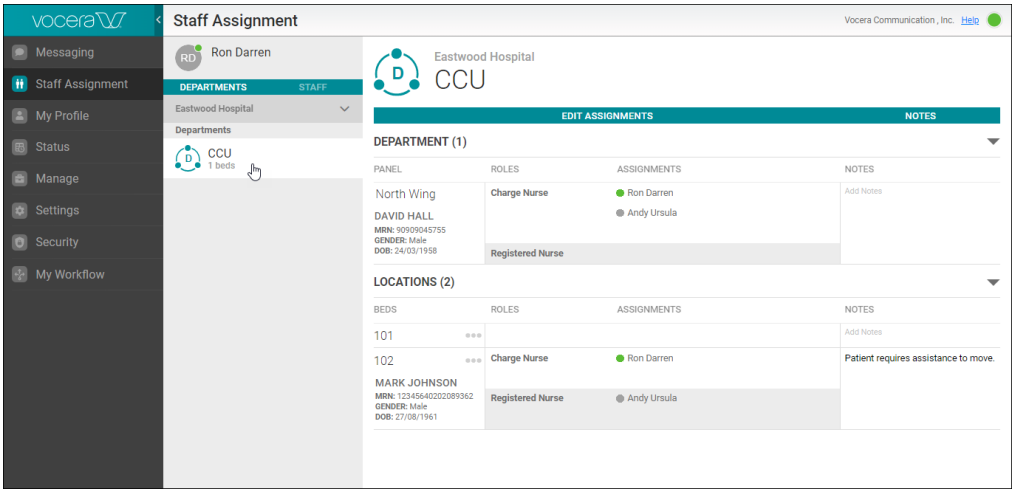
This topic describes the steps to view the departments within a facility.

To view departments within your facility, do the following:

1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff in the default department.



2. Click **DEPARTMENTS** to view the departments within your facility.
   The list of departments within the facility are displayed.

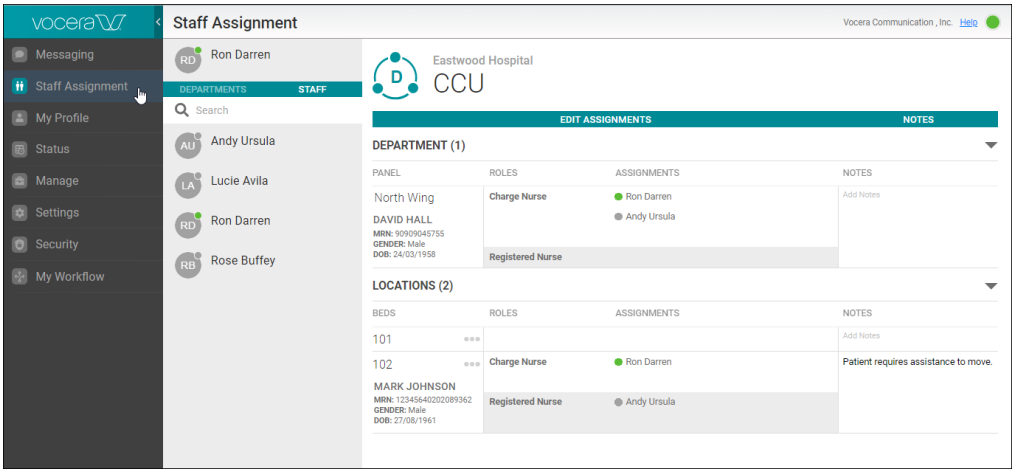


Setting a Department to Home Department

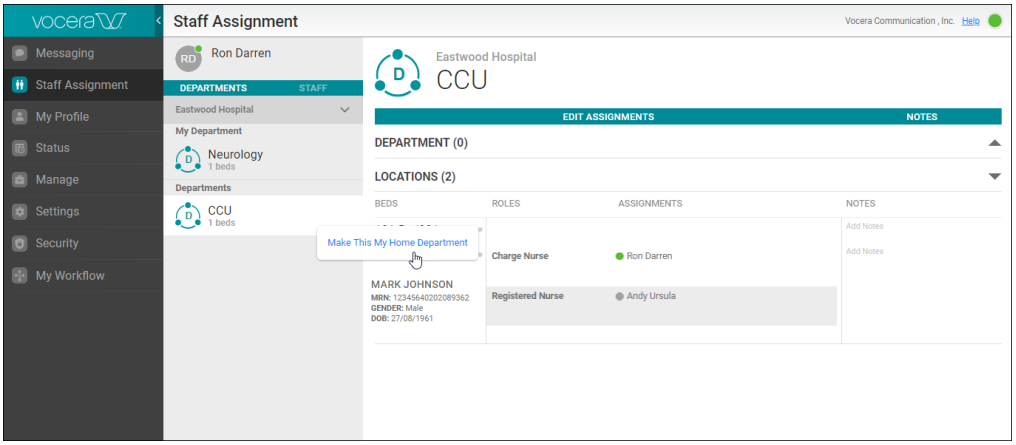
This topic describes the steps to set a department as a home department.

To set a department to home department, do the following:

1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff in the default department.



2. Click **DEPARTMENTS** to view the departments within your facility.
   The list of departments within the facility are displayed.
3. Right click a department and select the option **Make This My Home Department**.

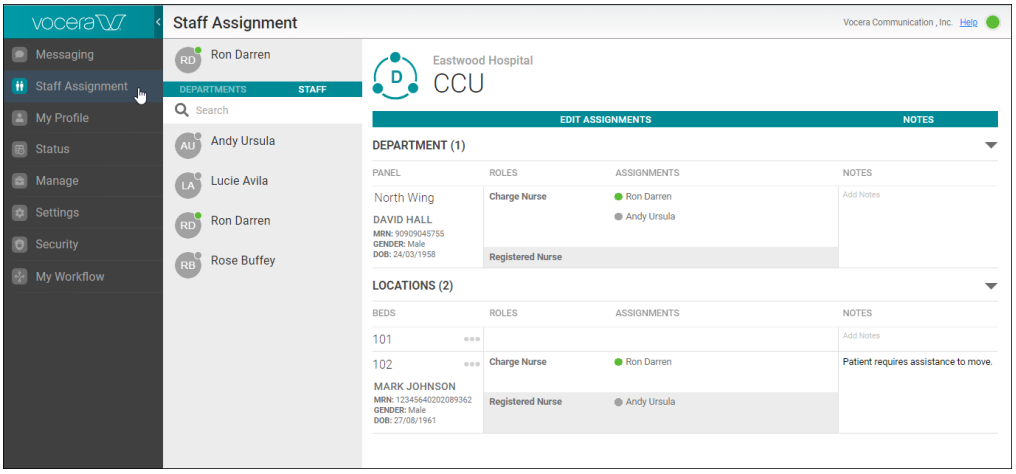


Viewing and Searching Staff Members

This topic describes the steps to view and search the staff members within a department or all departments in a facility.

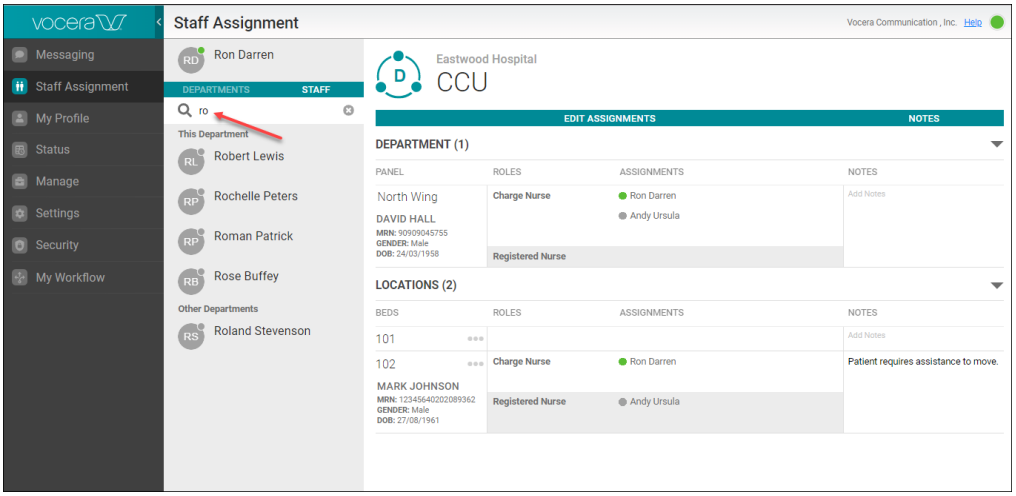
To view staff members within your facility, do the following:

1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff in the default department.



2. Type the name of the staff or the beginning two letters of the staff name that you want to search in the **Search** field.
   All staff names that contain the searched letters or word are listed.

Note: The search result lists all staff names across departments within a facility.

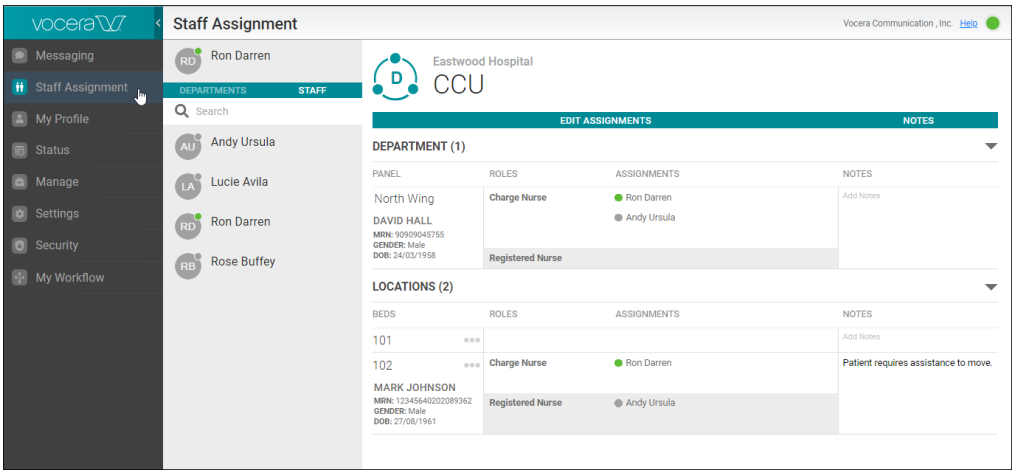


Assigning Staff Member by Clicking

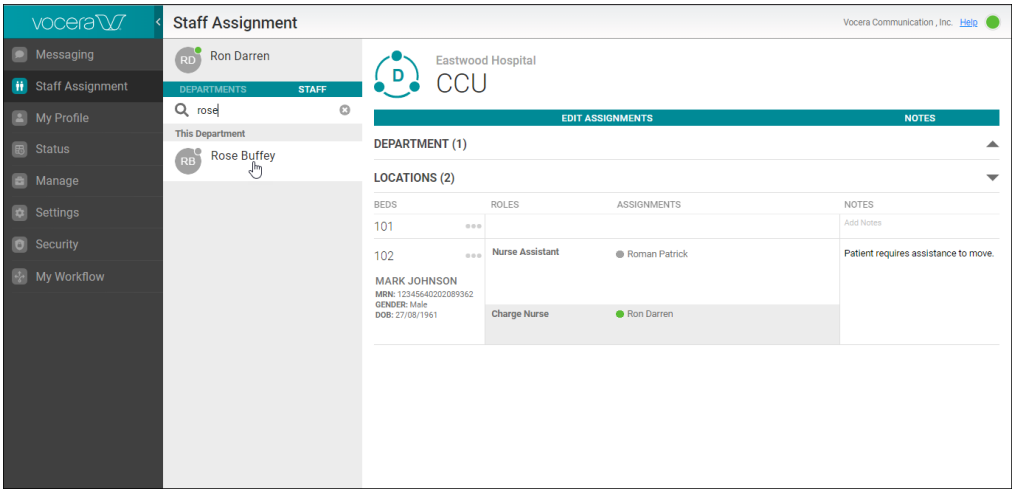
This topic describes the steps to assign a staff member by clicking the name of a staff member.

To assign a staff member by clicking, do the following:

1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff members in the default department.

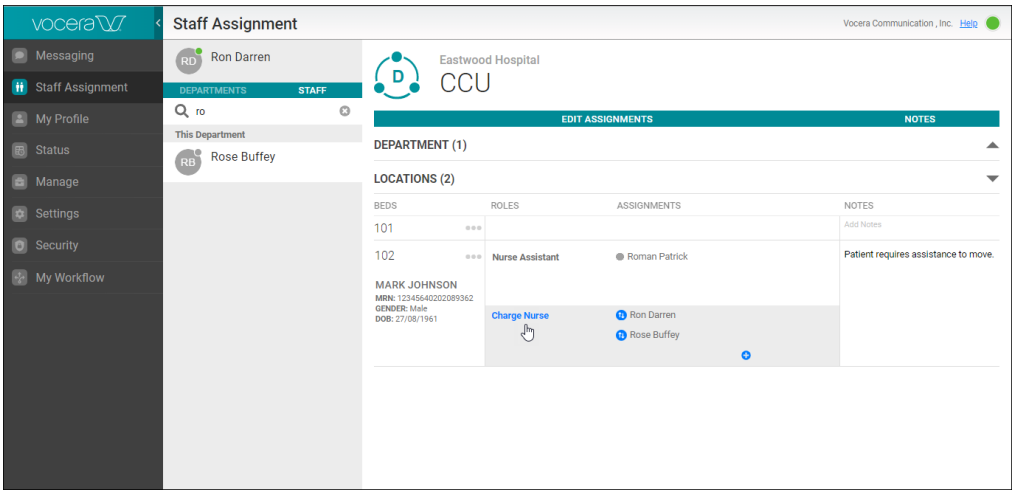


2. In the **STAFF** tab, click the name of the staff member that you want to assign to a patient. For example, **Rose Buffey**.



3. In **EDIT ASSIGNMENTS** tab, click the role that you plan to assign to the selected staff member. For example, click **Charge Nurse**.

   The selected staff is assigned the role of Charge Nurse. In this example, Rose Buffey is assigned as a charge nurse to the patient Mark Johnson.



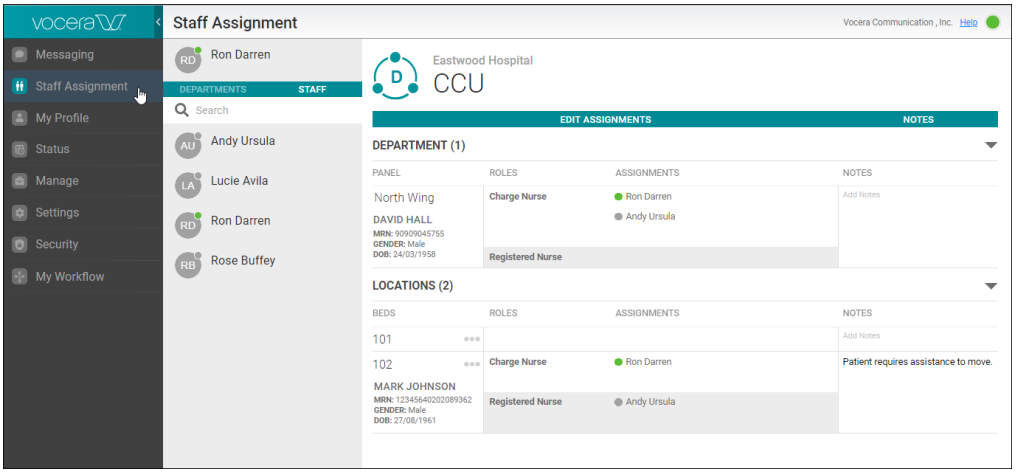
Assigning Staff Member by Replacing

This topic describes the steps to assign a staff member by replacing an assigned staff member.

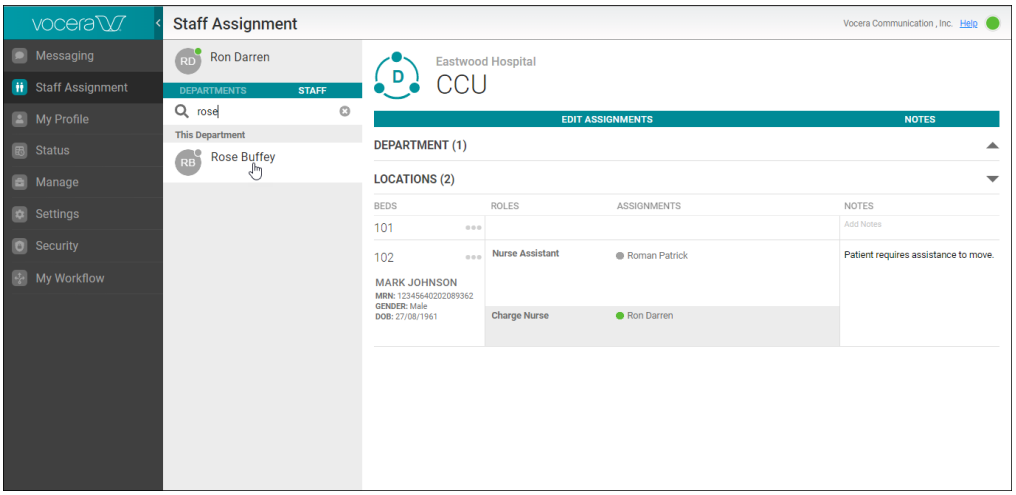
To assign a staff member using replace, do the following:

1. Navigate to **Staff Assignment** module.

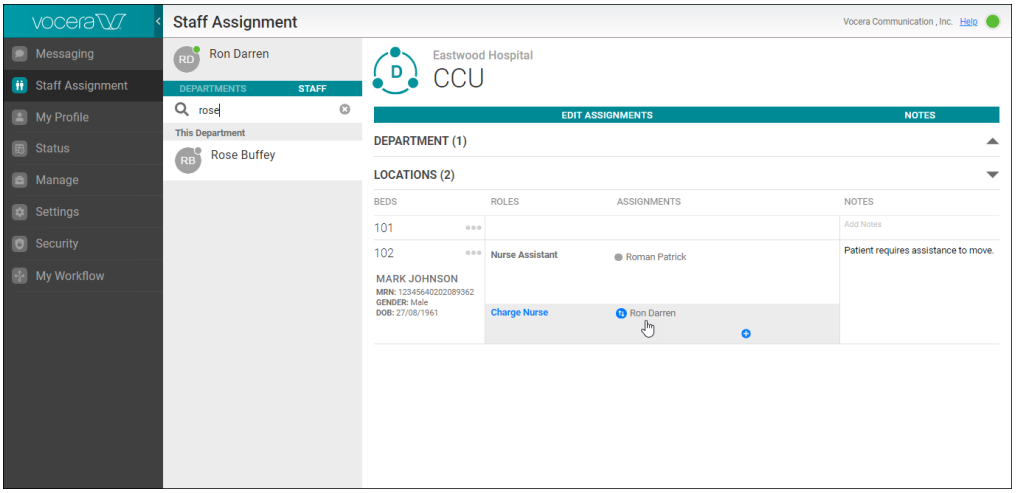
   The Staff Assignment page opens and lists the names of the staff members in the default department.



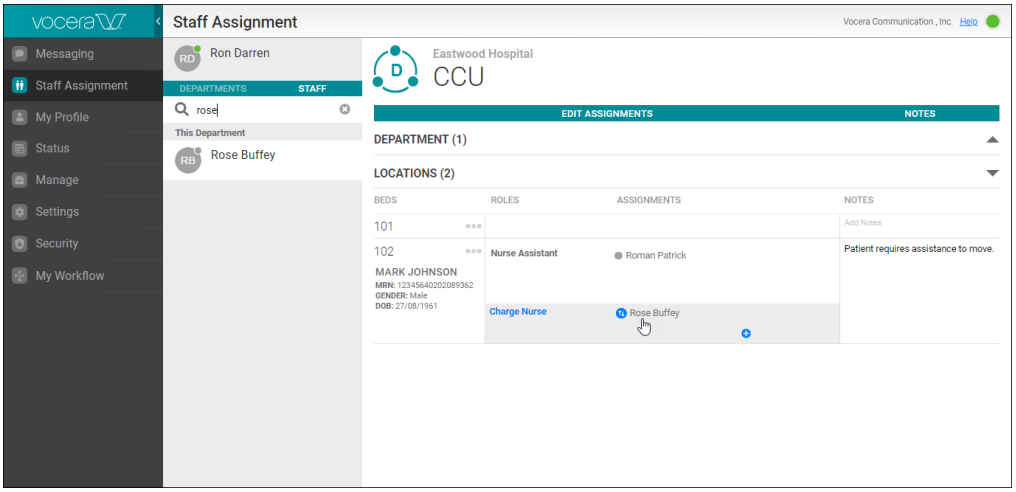
2. In the **STAFF** tab, click the name of the staff member that you want to assign to a patient. For example, **Rose Buffey**.



3. In **EDIT ASSIGNMENTS** tab, click the staff member that you plan to replace with the selected staff member. For example, click **Ron Darren**.



The selected staff member is replaced the new staff member. In this example, **Ron Darren** is replaced with **Rose Buffey**.

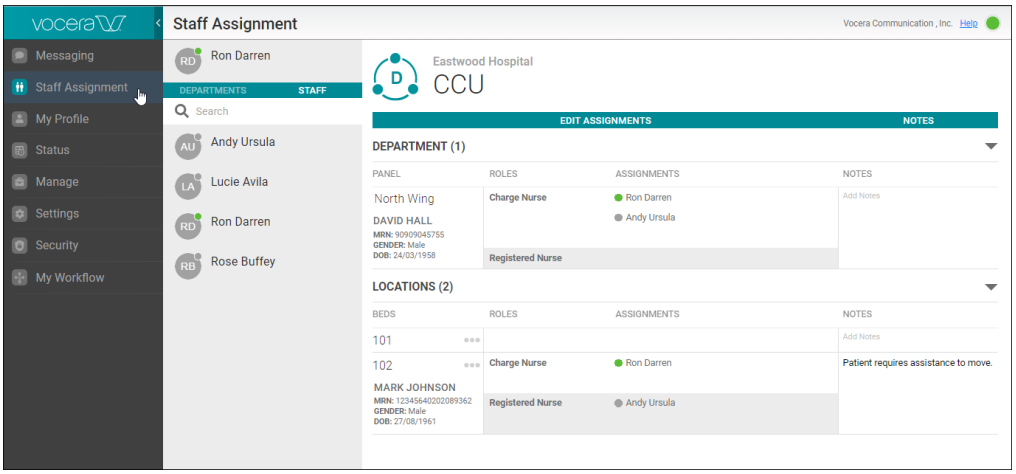


Assigning Staff Member by Typing

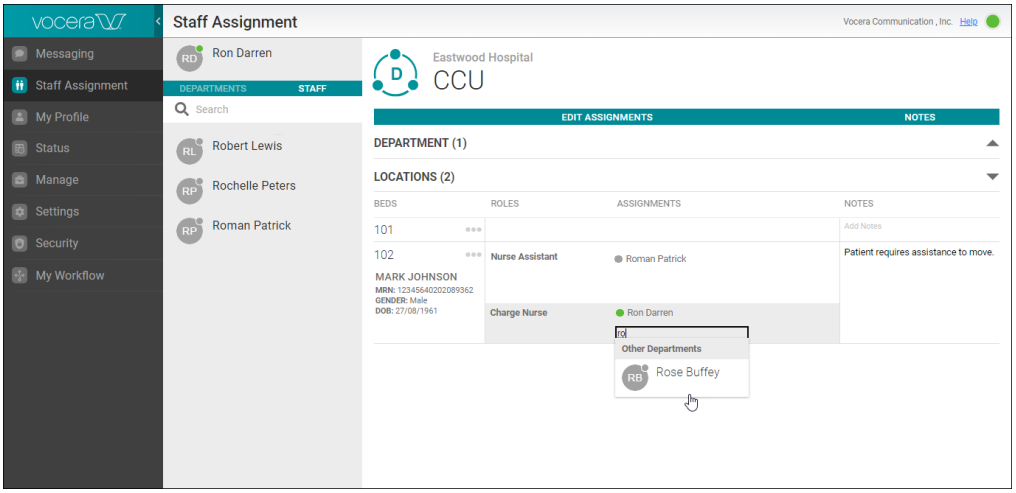
This topic describes the steps to assign a staff member by typing the name of a staff member.

To assign a staff member by typing a staff member name, do the following:

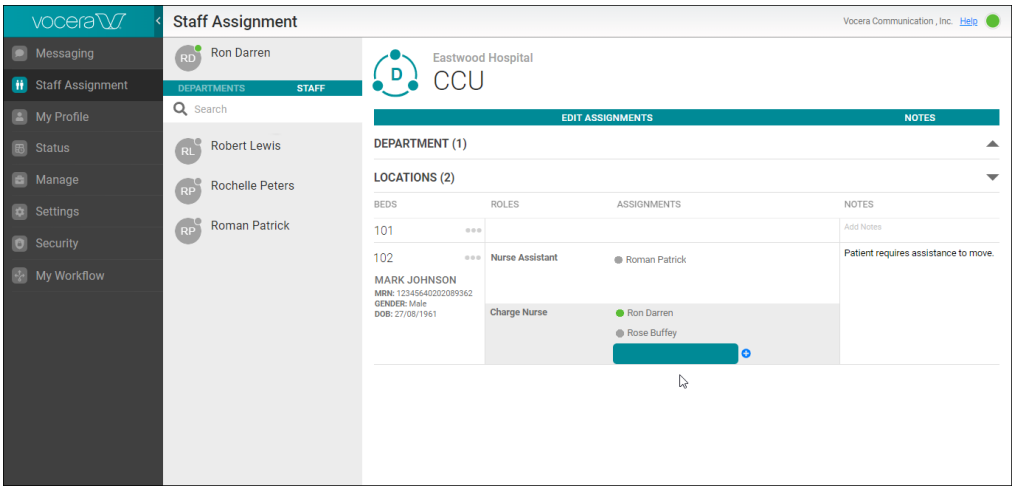
1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff members in the default department.



2. In **EDIT ASSIGNMENTS** tab, under Assignments column, type the name of a staff member. For example, type **rose**.
   The names of staff members that contain the word **rose** are populated automatically.



3. Select the name of the staff member that you intend to assign. For example, select **Rose Buffey**.
   The selected staff member is assigned to the respective patient.

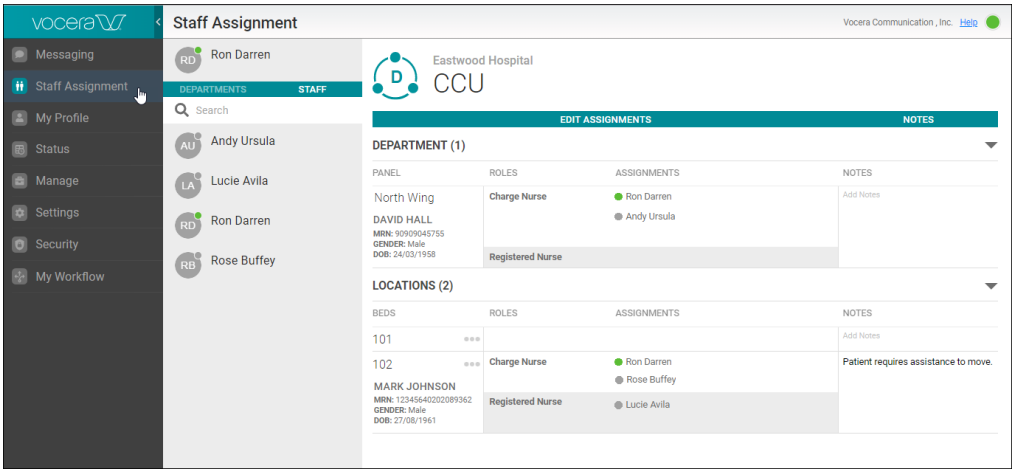


Assigning Staff Member using Copy and Paste

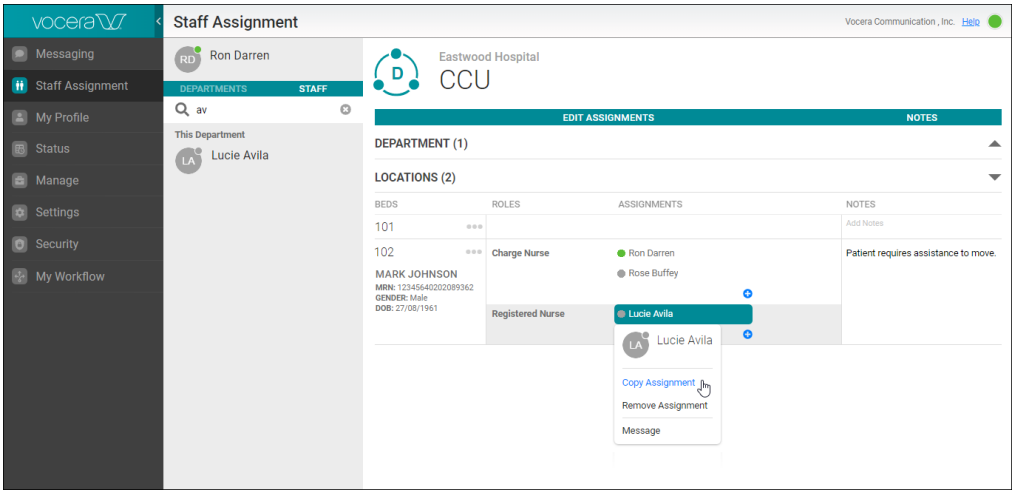
This topic describes the steps to assign a staff member using copy and paste.

To assign a staff member using copy and paste, do the following:

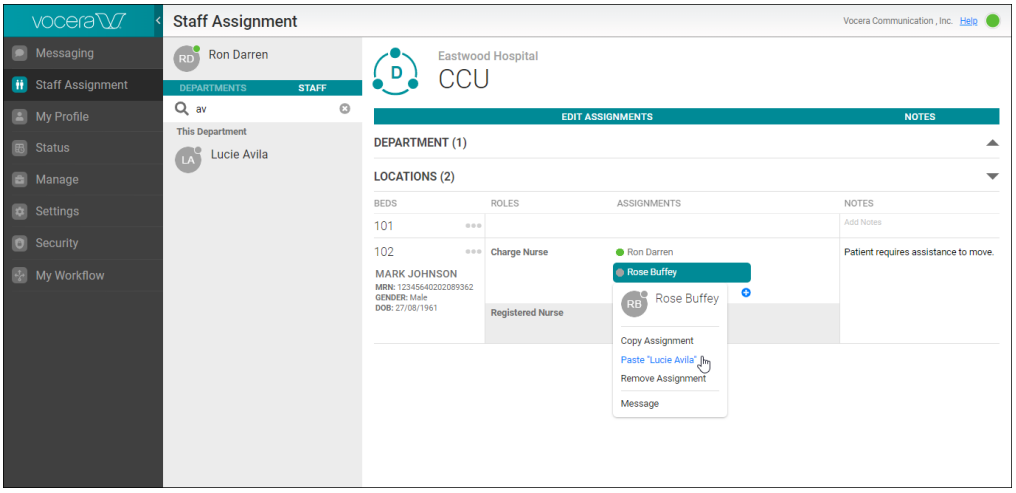
1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff members in the default department.



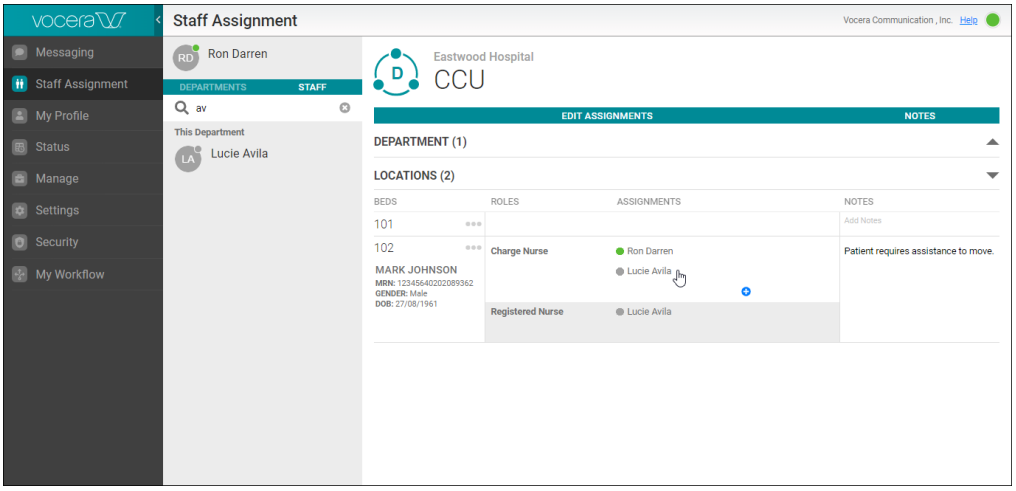
2. In the **EDIT ASSIGNMENTS** tab, right click the name of the staff member that you want to copy and select **Copy Assignment** or select the cell and press `Ctrl+C`. For example, **Lucie Avila**.



3. Right click on the staff member name that you want to replace the copied staff member,or select the cell and press `Ctrl+V`. For example, **Rose Buffey**.



4. Click **Paste** '**Lucie Avila**' from the dropdown list.
5. The existing staff member is replaced with the copied staff member.
   For example, **Rose Buffey** is replaced with **Lucie Avila**.

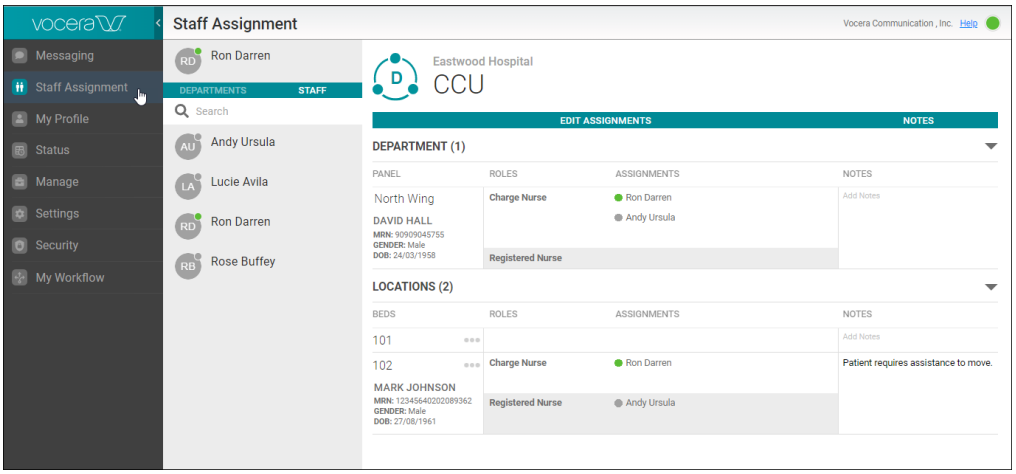


Messaging Care Team

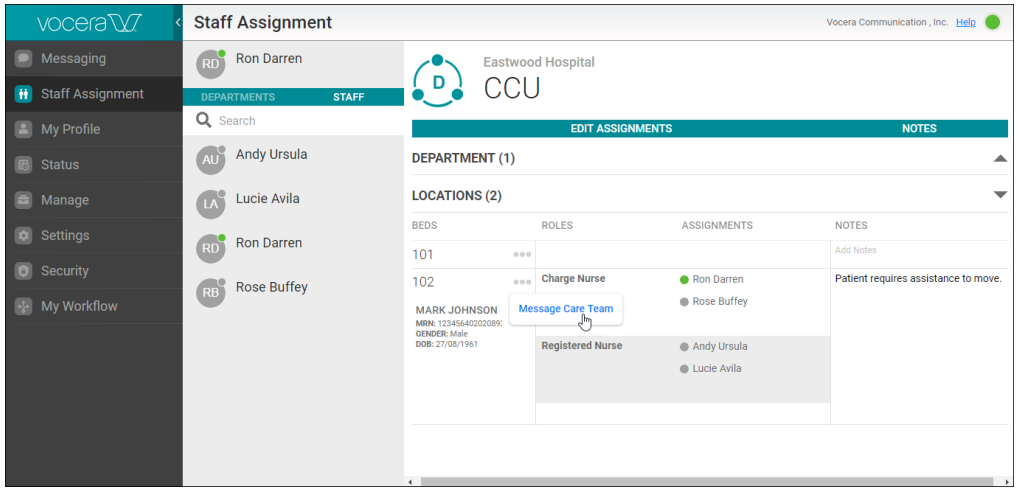
This topic describes the steps to send a message to the Care Team.

To send a message to the Care Team, do the following:

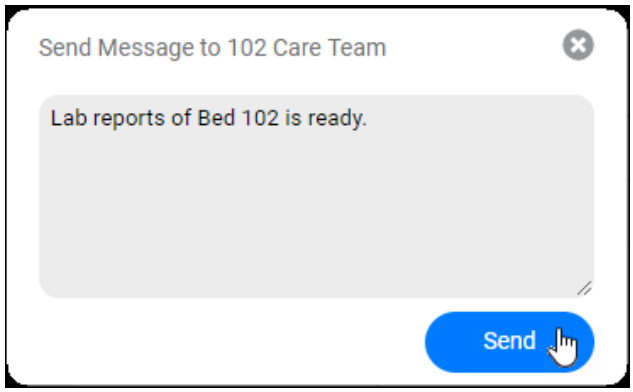
1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff members in the default department.



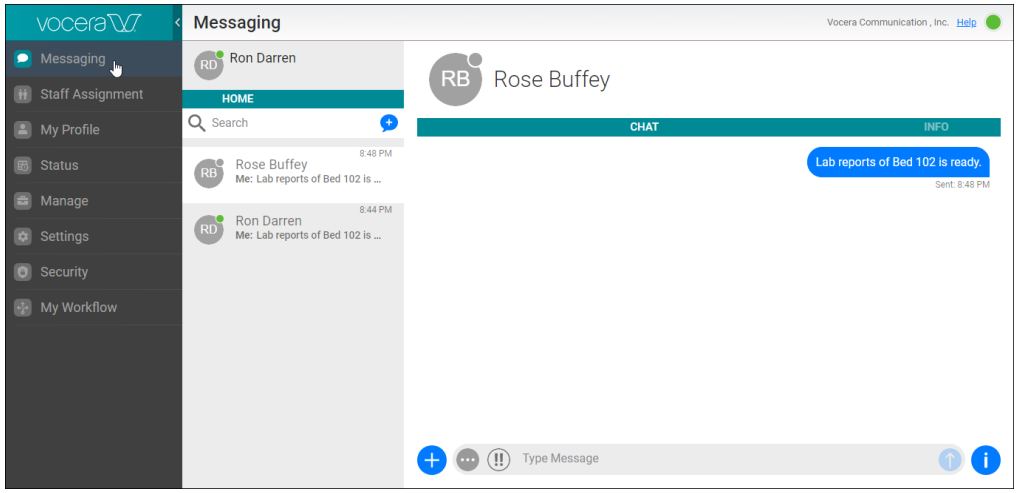
2. In **EDIT ASSIGNMENTS** tab, click the three dots displayed next to the Bed number.
   The **Message Care Team** option is displayed.



3. Click **Message Care Team**.
   The message dialog box opens.



4. In the message dialog box, enter the message you intend to send to the Care Team. For example, **Lab reports of Bed 102 is ready**.
5. Click **Send**.
   The message is sent to the Care Team.
6. Navigate to **Messaging** module.
   The Messaging page opens and lists the sent messages.
   The message sent to the Care Team is displayed along with the timestamp.

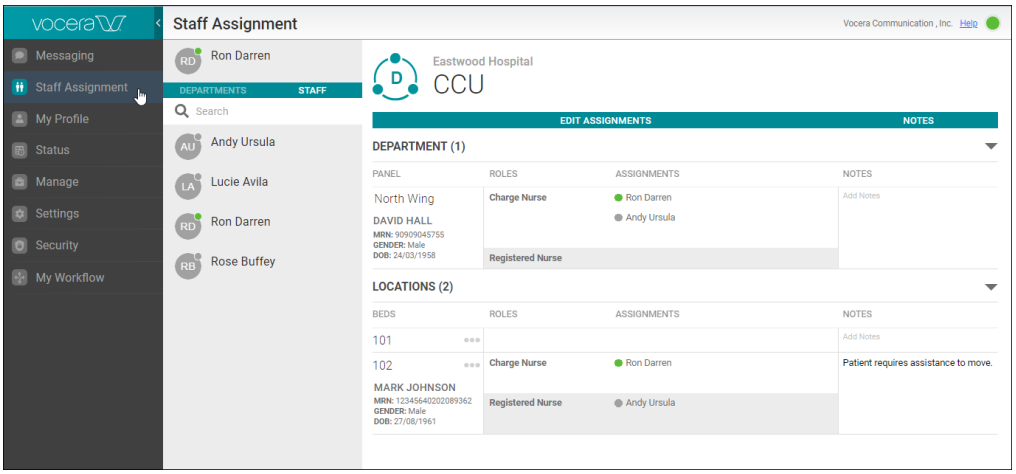


Messaging an individual Staff Member

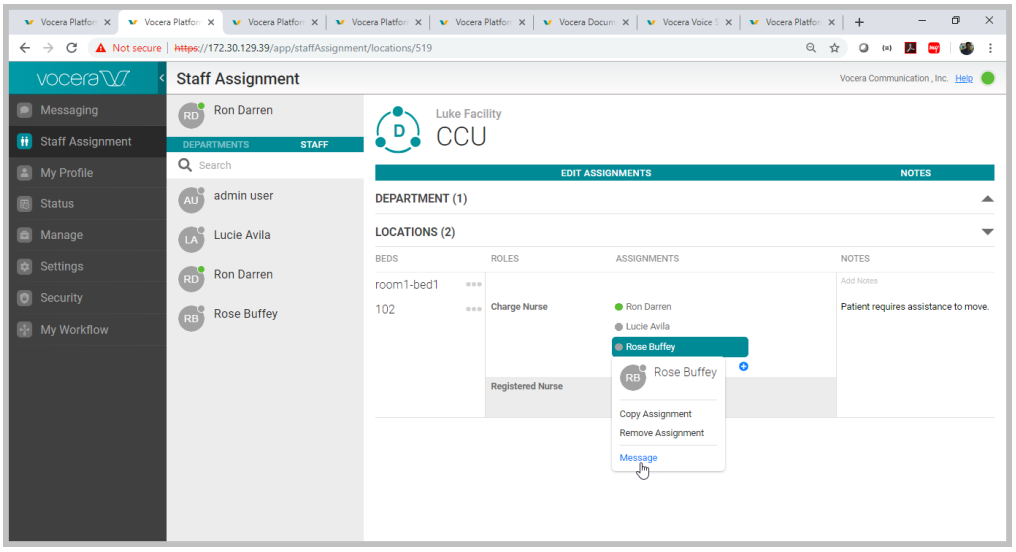
This topic describes the steps to send a message to an individual staff member.

To send a message to an individual staff member, do the following:

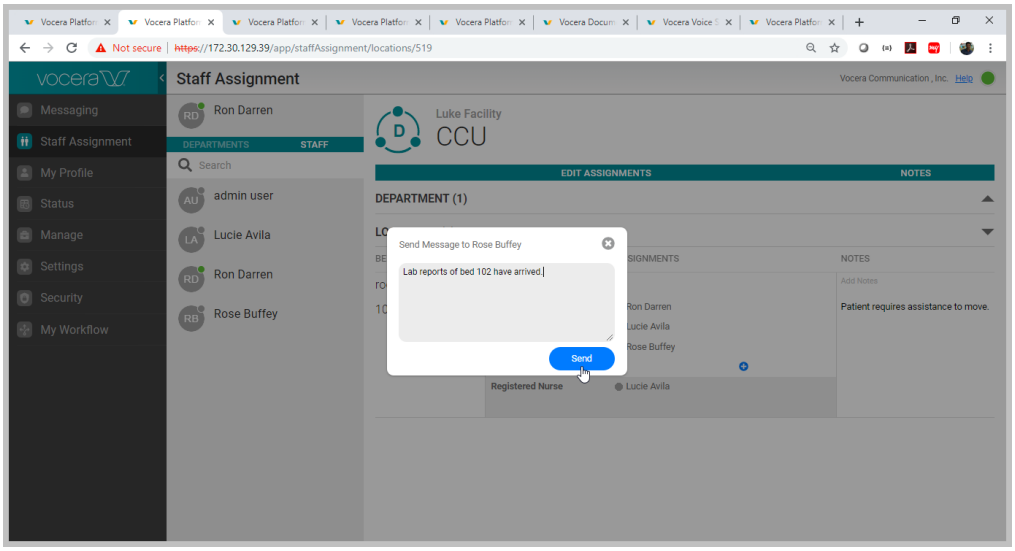
1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff members in the default department.



2. In **EDIT ASSIGNMENTS** tab, right click the staff member that you intend to send a message to display the dropdown options. For example, right click **Rose Buffey**.
3. Click **Message** from the dropdown list.
   The message dialog box opens.



4. In the message dialog box, enter the message you intend to send to the individual. For example, **Lab reports of Bed 102 have arrived.**



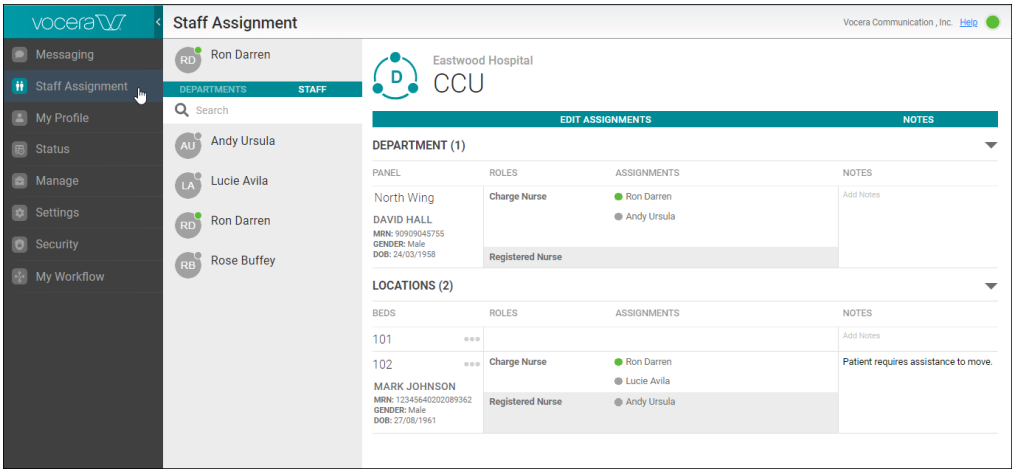
5. Click **Send**.
   The message is sent to the recipient.

Removing a Staff Assignment

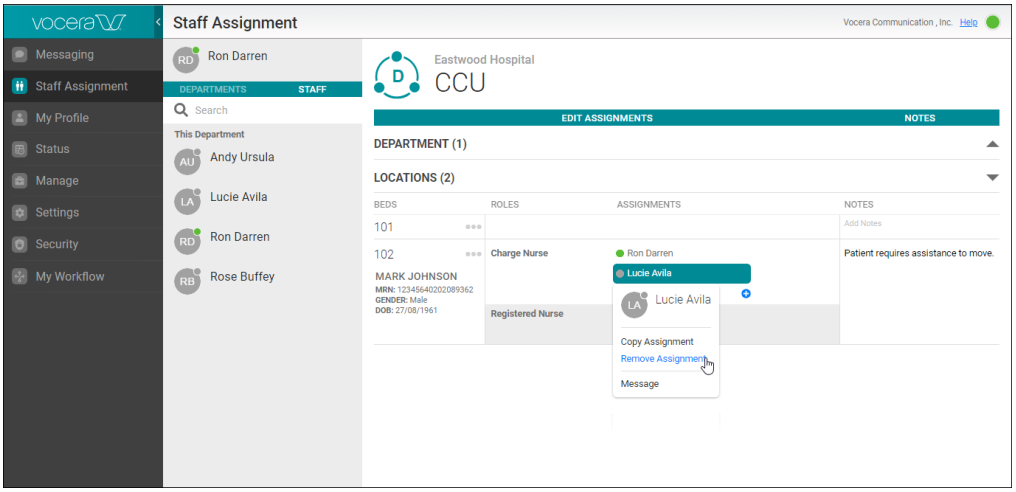
This topic describes the steps to remove staff assignment for an already assigned staff member.

To remove staff assignment role for an assigned staff member, do the following:

1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff members in the default department.



2. In **EDIT ASSIGNMENTS** tab, right click the staff member that you intend to remove staff assignment or select the staff member and click **Delete** on your keypad. For example, right click **Lucie Avila**.



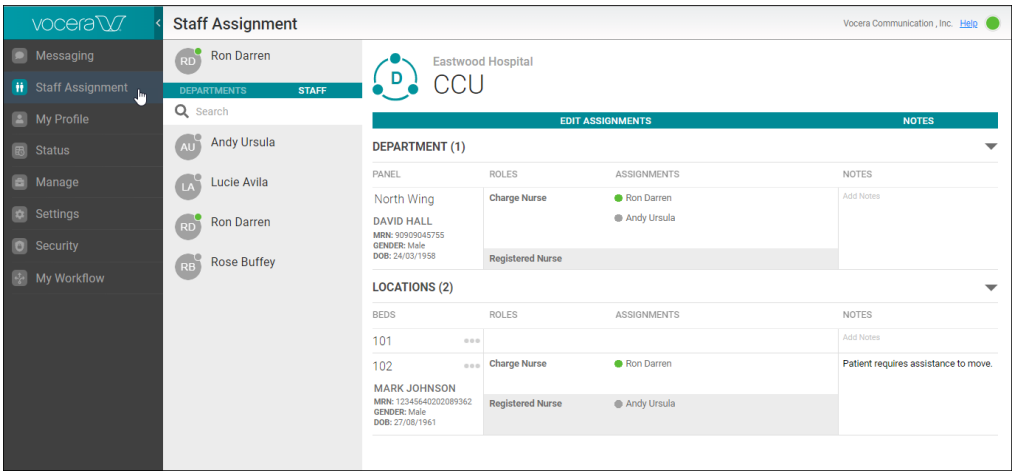
3. Click **Remove Assignment** from the dropdown list.
   The staff member, **Lucie Avila**, is removed from the respective assignment.

Adding Notes for a Patient

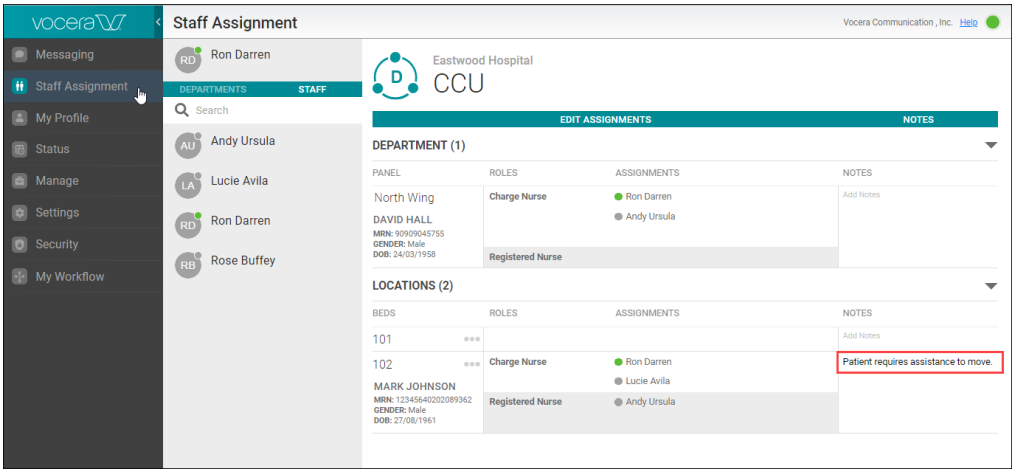
This topic describes the steps to add notes specific to a patient.

To add notes for a patient, do the following:

1. Navigate to **Staff Assignment** module.
   The Staff Assignment page opens and lists the names of the staff members in the default department.



2. In **EDIT ASSIGNMENTS** tab, under **NOTES** column, locate the **Add Notes** field and enter notes specific for the patient. For example, type **Patient requires assistance to move**.


vocera
Staff Assignment
Vocera Communication , Inc. Help
Messaging
Staff Assignment
My Profile
Status
Manage
Settings
Security
My Workflow
Ron Darren
DEPARTMENTS
STAFF
Search
Andy Ursula
Lucie Avila
Ron Darren
Rose Buffey
Eastwood Hospital
CCU
EDIT ASSIGNMENTS
NOTES
DEPARTMENT (1)
PANEL
ROLES
ASSIGNMENTS
NOTES
North Wing
DAVID HALL
MRN: 90909045755
GENDER: Male
DOB: 24/03/1958
Charge Nurse
Ron Darren
Andy Ursula
Add Notes
Registered Nurse
LOCATIONS (2)
BEDS
ROLES
ASSIGNMENTS
NOTES
101
Add Notes
102
Charge Nurse
Ron Darren
Lucie Avila
Patient requires assistance to move.
MARK JOHNSON
MRN: 12345640202089362
GENDER: Male
DOB: 27/08/1961
Registered Nurse
Andy Ursula

My Profile

The My Profile section in the Vocera Platform Web Console navigation bar allows you to manage your profile information and customize your voice and speech recognition settings.

- About the Vocera Platform My Profile Guide on page 80
- The My Profile Home Page Layout on page 81
- Working With My Profile on page 83

About the Vocera Platform My Profile Guide

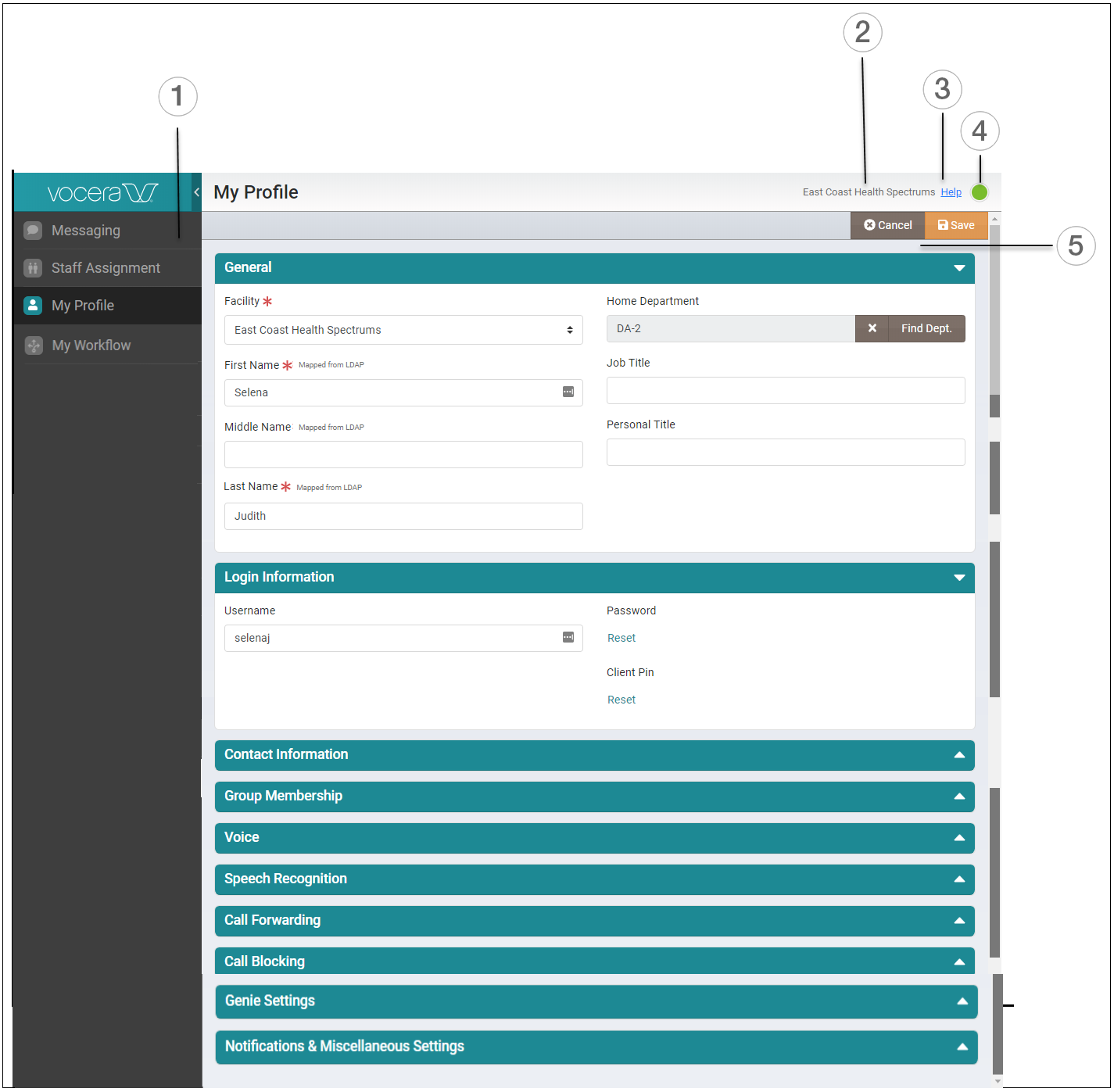
The Vocera Platform My Profile Guide describes how to perform tasks using the My Profile application.

You can use this document as you work with My Profile, and you can get the same information from the console's context-sensitive help. The organization of this guide follows the layout of the My Profile console.

The My Profile Home Page Layout

After you log into to My Profile, you see the Home page with configuration fields that you can use to view and customize your settings and preferences.

The following screenshot shows My Profile Home page:



The following table describes the user interface elements in the Vocera Platform My Profile

Numbers	Descriptions
1	The navigation bar with various sections supported in theMy Profile Web Console.
2	The name of your company.
3	The weblink to the My Profile context-sensitive help.
4	The Presence icon.
5	The My Profile configuration section.

Working With My Profile

Use the My Profile Web Console to view and customize your profile information, settings, and preferences related to Vocera devices and mobile applications.

The My Profile is a Web application hosted on the Vocera Platform.

The profile information registers you as a user on the system, and stores permissions and preferences that control how your Vocera devices and mobile applications work. Your profile information is stored in a database on the Vocera Platform.

Viewing and Editing General Profile Information

View and edit your basic profile information in the General section.

You can edit your First Name, Last Name, Job Title, and Personal Title from the General section.

1. In the General section, complete the fields listed in the table below. An asterisk * indicates that a value must be entered for this field.

Field	Maximum Length	Description
Facility *	50	Displays the facility that represents your physical location. If you do not have a specific facility associated with your profile, the default **Global** facility is displayed. If you have multiple facilities associated with your profile, you can click on the Facility field arrowhead to toggle between the facilities.
First Name *	50	Displays your first name. This field is auto populated if your Vocera system is integrated with your organization's Active Directory. You can change your first name and enter a new first 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 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 section.
Middle Name	50	(Optional) Enter the user's middle name. The middle name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed.
Last Name *	50	Enter the user's last name. The last name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed.

Field	Maximum Length	Description
Home Department	50	Displays the home department assigned by your system administrator. If you don't have an assigned home department, click **Find Dept.** to display the Find a Department dialog box,and select a home department from the list. If your organization has multiple facilities connected to the same Voice Service, choose the facility that represents your physical location.
Job Title	100	(Optional) Enter a job title for the new user. Provide the full spelling of the title rather than an abbreviation. For example, enter Professor instead of Prof.
Personal Title	100	(Optional) Enter a personal title for the new user. For example, Mr., Ms., Mrs.

2. Select one of the following from the top right hand corner of the My Profile:
   - **Save** — to save your changes.
   - **Cancel** — to exit the General section without saving any changes.

Viewing and Editing Login Information

View and edit your login information in the Login Information section of the My Profile Web Console

You can view your Username and reset your Client Pin and Password information from the Login Information section.

1. In the Login Information section, view the fields listed in the following table:

Field	Maximum Length	Description
Username *	50	Displays your **My Profile** username. The minimum length for username is 4 characters and maximum is 50 characters. You can only use letters, digits, underscores (_), or dashes (-) in your username. No other characters are allowed.
Password Reset	64	Displays your **My Profile** login password. The minimum length for password is 4 characters and maximum is 64 characters. You can use alphabets, numbers, common punctuations, and symbols in your password. No other characters are allowed. **Note:** Depending upon the permissions associated with your role, you may or may not see this field in the Login Information section.
Client Pin Reset	Varies per PIN policy	Allows to reset an existing Client Pin and add a new Client Pin on your Vocera device.

2. (Optional) Click the **Password Reset** field to reset your password.
   Click Reset Password link to display the Reset Password dialog box.
   1. Specify a new password in the **New Password** field.
   2. Re-enter this password in the **Repeat Password** field.
   3. Select **Reset** to proceed with the password reset action.
3. (Optional) Click the **Client Pin Reset** field to reset your Vocera device PIN.
   Click Reset Client Pin link to display the Reset Client Pin dialog box.
   1. Specify a client pin in the **New Client Pin** field.
   2. Re-enter this pin value in the **Repeat Client Pin** field.
   3. Select **Reset** to proceed with the client pin reset action.
4. Select one of the following:
   - **Save** — to save your changes.
   - **Cancel** — to exit the Login Information section without saving any changes.

Adding Contact Information

Use the fields in the Contact Information section to enter your contact details.

If this field is pre-populated with some data, you can edit this information as needed.

1. In My Profile scroll down to the Contact Information section and click the drop down arrow at the right hand side to expand this section.
2. Complete the field information as described in the following table:

Field	Maximum Length	Description
Email Address	60	Enter the contact email address to facilitate the following: Other users can send voice messages from their devices 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. .
Cell Phone	50	Allows users to forward calls from a device 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 devices to their home phones. It also allows users to take advantage of the "Call My House" Contacts entry.
Employee ID	50	Specify an employee ID (unique value) that identifies a Vocera user. **Note:** You must have System Administrator or Tiered Administrator privileges to change or enter the Employee ID.
Desk Phone or Extension	50	Enables the following features: • Allows you to forward or transfer calls from your Vocera devices to your desk phones. • If no Vocera Extension is specified, outside callers can connect to your Vocera device by entering your desk extension at the Vocera hunt group prompt, instead of saying/speaking your name. • Allows you to send a page and receive the return phone call from a person you paged on your device. • If you have appropriate permission and have Vocera Access Anywhere enabled, the Desk Phone or Extension field allows you to be authenticated by Caller ID when you call the Vocera hunt group number.
Pager	50	Allows you with the proper permissions to receive numeric pages on your pagers from other device users who issue the "Page" voice command.
Cost Center	100	Displays the cost center to which you are assigned. A cost center ID lets Vocera track system usage by users and potentially allows an organization to charge for relative usage.

3. Select one of the following:
   - **Save** — to save your changes.
   - **Cancel** — to exit the Contact Information section without saving any changes.

Viewing Group Membership

Use the fields in the Group Membership section to view your group membership information.

1. In My Profile scroll down to the Group Membership section and click the drop down arrow at the right hand side to expand this section.
2. In the Group Membership section, view groups for which you have a membership.

Note: The values in the **Group Name** and **Facilities** fields are greyed out to indicate that you cannot change them. Only the Vocera System Administrator can change the name of a group or the facility information.

3. (Optional) Click **Add Group** to display the Select Group dialog box.
   The Select Group dialog box displays a list of Groups and Facilities that you add yourself to. If you add yourself to a group in a specific facility, click **Save** on the top right hand corner of the My Profile to make sure that your changes are saved in the system.
   a. Select a group name from the list of groups displayed.
   b. Click **Select Groups** or **Cancel** to close the dialog.
4. In the **Conference Group this user is a member of** field, view the names of the Conference Groups to which you belong.
   You can only belong to one conference at a time even if you are a member of multiple groups.

Adding Groups

Use the fields in the Group Membership section to add groups.

Important: Not all users have the required permission to add a group. Contact your system administrator to learn more about permissions related to your user account.

1. In My Profile scroll down to the Group Membership section and click the drop down arrow at the right hand side to expand this section.
2. Click **Add Group** to display the Select Group dialog box.
   The Select Group dialog box displays a list of Groups and Facilities that you can add yourself to or become a member of.
3. Select a group name from the list of groups displayed.
4. Click **Select Groups** or **Cancel** to close the dialog.
5. If you add yourself to a group in a specific facility, click **Save** on the top right hand corner of the My Profile to make sure that your changes are saved in the system

Removing Groups

Use the fields in the Group Membership section to remove groups.

Important: Not all users have the required permission to remove all groups. Contact your system administrator to learn more about permissions related to your user account.

1. In My Profile scroll down to the Group Membership section, and click the drop down arrow at the right hand side to view all the groups that you have membership.
2. Click the **Delete** icon next to the group that you wish to delete.

3. Select one of the following from the top right hand corner of the My Profile page:
   - **Save** — to save your changes.
   - **Cancel** — to cancel the delete action.

Viewing and Configuring Voice Service Fields

Use the fields in the Voice section to enter and view the Voice Service related information.

If the fields in this section are pre-populated with some data, you can edit this information as needed.

1. In My Profile scroll down to the Voice section and click the drop down arrow at the right hand side to expand this section.
2. In the Voice section, complete the fields described in the following table:

Field	Maximum Length	Description
Vocera Phone	50	Specify the Vocera phone information to forward calls from your Vocera devices to the specified phone number. You can route calls made to this virtual extension to go to your 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 your desk phone to be routed to the your Vocera device. Because the Vocera extension is a virtual phone number, you can put any number in the Vocera Extension field. If you already have 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 the dynamic extensions feature is enabled. Similarly, this field may continue to display an expired number that has not been reassigned; you can keep the number as long as it is available.
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 facilities. A PIN template can include digits, special characters, and PIN macros.

Field	Maximum Length	Description
Device ID	12	Enter the MAC address of the device. This is available on the device's **Info** menu. The MAC address of a device is also printed near the bottom of the white label under the battery.For Vocera devices, 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.
Enable Access Anywhere	n/a	Allows you to access the Vocera 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. If this feature is disabled for you, contact your system administration for information on enabling this feature and further guidelines.
Phone Password	25	Specify the password used to authenticate the user when accessing the Vocera Genie from a phone. The Phone Password must be five to 25 characters consisting of letters or numbers. Special characters are not allowed.
Repeat Phone Password	25	Re-enter the password that you entered in the **Phone Password** field.

3. Select one of the following:
   - **Save** — to save your changes.
   - **Cancel** — to exit the Contact Information section without saving any changes.

Configuring Speech Recognition

Use the Speech Recognition fields to enter variations of your name, to increase the Vocera Genie's ability to recognize you when someone is speaking your name.

Speech Recognition fields are useful when another user issues a command to call you, leave a message for you, locate you, and so forth. The Vocera system software analyzes the name the caller spoke and matches it to the text in the First Name and Last Name fields of your profile.

1. In My Profile scroll down to the Speech Recognition section and click the drop down arrow at the right hand side expand this section.
2. Complete the field information as described in the following table:

Field	Maximum Length	Description
Doctor Prefix	n/a	Select the Doctor Prefix check box to indicate the user is a Doctor. If you are using this option, you do not need to enter Doctor prefix as a value for one of the **Alternate Spoken Name** (ASN) fields. For example, if you selected **Doctor Prefix** field for a user named, "John Smith," you can use a voice command, "Call Dr Smith" on your device. Vocera speech recognition will quickly recognize this voice command and call the user named John Smith.
Enable Frequently Called User	n/a	Select Enable Frequently Called User checkbox to include yourself in the weighing for improving speech recognition for frequently called users and departments. If you do not select this checkbox, you are excluded from the weighing for improving speech recognition for frequently called users and departments.

Field	Maximum Length	Description
Alternate Spoken Name #1	50	Enter an alternate spoken name. By default, it is assumed that you are called by either your first and last name. Enter an Alternate Spoken Names only if: • People call you with different names (such as "Bill Smith" in addition to "William Smith") • Your name is pronounced differently from the way that it is spelled. In this case, add one or more phonetic spellings. Use these guidelines to ensure the best result when you are defining alternate names for users: • **Person, Group, and Location Names** — If users refer to a person, group, or location 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. • **Digits in Name Fields**— 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 these special characters are allowed, it is unlikely that an alternate spoken name would need underscores (_), or dashes (-). • **Staff IDs** — It is recommended that you do not create an alternate spoken name that contains numeric digits only. For example, a staff ID with numbers and no letters. 567748 Entering numeric staff IDs are permitted. However, using numeric values only might result in • Slower Genie response times • Problems with phone number recognition • **Acronyms and Initials in Alternate Spoken Names**— If people use an acronym or initials to refer to a Contacts 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. For Jasdeep Narindar Singh, also enter J N Singh rather than J.N. Singh. • **Unusual Pronunciation**— If a name has an unusual or confusing pronunciation or silent letters, 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. • **Professional Titles in Alternate Spoken Names**— If users refer to a person by his or her title, provide the full spelling of the title rather than an abbreviation. For example, enter Father Brown instead of Fr. Brown, or Professor Lindsay instead of Prof. Lindsay. • **Doctor Title in Alternate Spoken Names**— When adding or editing user profiles, you do not need to include the Doctor title as part of the user's name in the Alternate Spoken Names (ASN) field on the Speech Recognition tab. Instead, check the Doctor Prefix check box. When you speak a command using one of the ASN variations, Vocera understands the user to whom you are referring. For example, when you speak, Call Doctor Michael Smith, the Vocera Genie knows that you are referring to Doctor Michael Smith. You could also speak, Call Doctor Smith or Call Doctor Michael and the Genie will find the user because the Doctor Prefix option is checked.
Alternate Spoken Name #2	50	The second alternate spoken name, if needed.
Alternate Spoken Name #3	50	The third alternate spoken name, if needed.
Identifying Phrase	100	Specify a phrase that distinguishes you from others with the same first and last names or name that sounds like your name. For example, "Bill Smith in Marketing." and "Bill Smith in Finance"

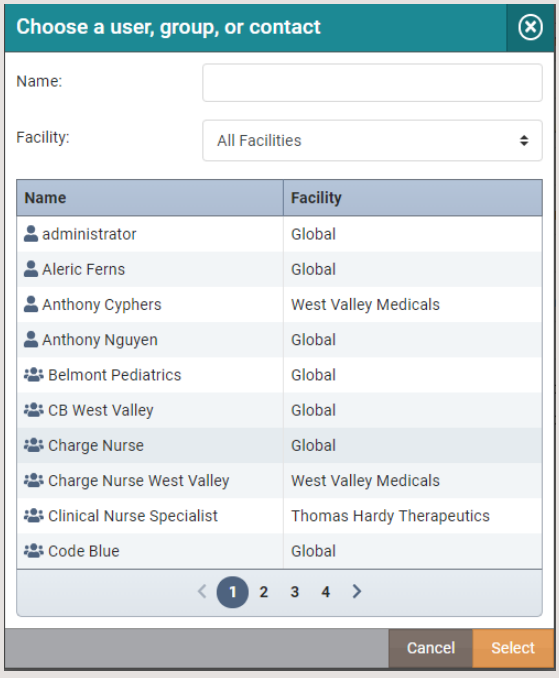
3. Select one of the following:
   - **Save** — to save your changes.
   - **Cancel** — to exit the Speech Recognition section without saving any changes.

Configuring Call Forwarding

Use the configuration fields in the Call Forwarding section to specify your call forwarding options and conditions.

Forwarding calls is helpful when you cannot answer a call for any reason, or when you block all calls or put your device in Do Not Disturb mode; your caller is usually prompted to leave a message.

1. In My Profile scroll down to the Call Forwarding section and click the drop down arrow at the right hand side to expand this section.
2. Select the **Enable Forwarding** checkbox to see the forwarding related fields. Optionally, specify where incoming calls are to be forwarded.
3. Choose one of the options described in the following table to specify where incoming calls are forwarded:

Forwarding Options	Descriptions
Forward to Company Voice Mail (default)	Select to forward the unanswered call to your company voice mail.
Forward to Another User, Group, or Contact	Select to forward the unanswered call to another user, group, or contact. If you selected **Forward to Another User, Group, or Contact**, Click the **Choose** button to display the Choose a user, group, or contact dialog box with a list of all the choices available in the system.  You can enter the name in the **Name** field to search for a user, group, or contact that you want search in the system. You can also use the **Facility** field to toggle between multiple facilities available in your system and refine your search. Click **Select** or **Cancel** to close the dialog box.

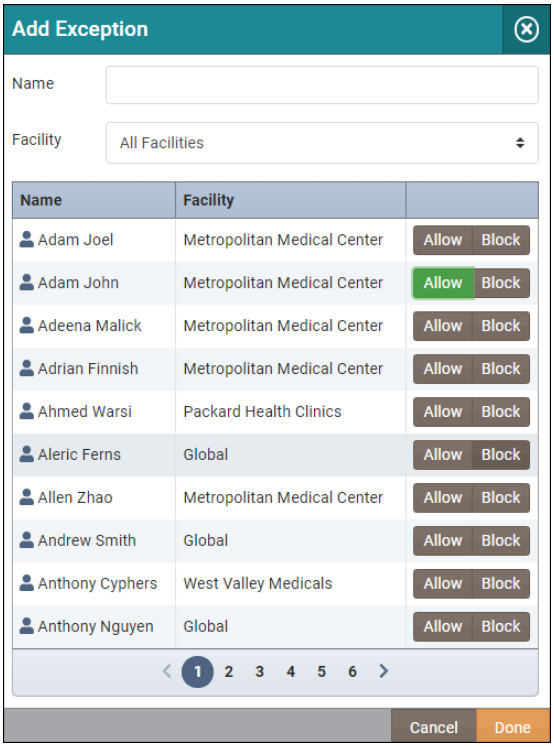
Forwarding Options	Descriptions
Forward to Desk Phone	Select to transfer the unanswered call to the desk phone number saved in the Contacts settings of the user's profile.
Forward to Cell Phone	Select to transfer the unanswered call to the cell phone number saved in the Contacts settings of the user's profile.
Forward to Home Phone	Select to transfer the unanswered call to the home phone number saved in the Contact's setting of the user's profile.
Forward to Another Number	Select to enter another number in the **Forward to Another Number** field.

4. Choose a condition to specify when to Forward the calls:
   - **All** — When selected, all calls are forwarded without an alert tone or ring on your device.
   - **Unanswered** — When selected, all unanswered calls are forwarded. This is also the system default.
   - **Offline** — When selected, forwarding occurs only when you are not logged in, or are off the network.
5. Select one of the following:
   - **Save** — to save your changes.
   - **Cancel** — to exit the Call Forwarding section without saving any changes.

Configuring Call Blocking

Use the configuration fields in the Call Blocking section to apply selective call screening and call blocking exceptions.

1. In My Profile scroll down to the Call Blocking section and click the drop down arrow at the right hand side to expand this section.
2. Select the **Block all calls by default** option.
   The **Allow all calls by default** option is selected as a default setting.
3. Click **Add Exceptions** to display the Add Exception dialog box.



4. Select the **Allow** or **Block** buttons next to caller names that you want to allow or block.
5. Choose one of the following to close the Add Exception dialog:
   - **Done** — to save the selections.
   - **Cancel** — to cancel the selections.
6. Select one of the following:
   - **Save** — to save your changes.
   - **Cancel** — to exit the Call Blocking section without saving any changes.

Configure Genie Settings

Use the Genie Settings section to configure the setting for Vocera Genie, which is the voice interface that you can use with the Vocera Platform.

The Vocera Genie is activated when you press the Call button on the Vocera devices and Genie icon on the mobile client applications. When the Genie is activated, it sends a greeting, accepts commands, and prompts you when necessary. When a call or a message comes to the Vocera device, the Genie notifies the recipient.

1. In My Profile scroll down to the Genie Settings section and click the drop down arrow at the right hand side to expand this section.
2. Complete the field information, as described in the following table:

Field	Description
Genie Voice	Click a radio button to choose a persona for Genie voice. You can click the preview icon by a persona name to play a sample. A Genie voice is a set of voice prompts and tones that give the voice interface a distinctive identity.

Field	Description
Genie Greeting	A Vocera device plays the Genie greeting when you press the Call button. Click a radio button to choose one of the following settings: • **Tone Only** • **Speech Only** • **Tone and Speech** Click the icon next to the choice to play a sample greeting. By default, the **Speech only** option is selected.
Call Announcement	In the **Call Announcement** section, choose a **Ring Tone** from the list. Click the icon next to the Ring Tone selector to play a sample. By default, the selected ring tone is Ring-Tone-01.
Announce caller's name after tone	Select the **Announce caller's name after tone** checkbox if you want to hear who is calling. This announcement adds to the time required to connect each call. By default, the **Announce Name of Called Group** box is selected.
Announce name of called group	Select **Announce Name of Called Group** if you want the Genie to identify the group that was called and the facility to which this group belongs (if it is different from the caller's facility). This helps in setting the context of the call for the recipient. For example, 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 facilities, the Genie says, "Call to [GroupName] at [FacilityName] from [CallerName]. Accept?" By default, the **Announce Name of Called Group** box is selected.

3. Select one of the following to close the dialog:
   - **Save** — to save your Genie Settings changes to the system.
   - **Cancel** — to discard all changes.

Notifications and Miscellaneous Settings

Use the Notifications and Miscellaneous Settings section to control the behavior of the alert tones, reminders that devices play and determine which automatic device features are enabled.

The Miscellaneous settings control the behavior of the "Play Messages" voice command, the behavior of call setup, and the enabling of Vocera Access Anywhere.

1. In My Profile scroll down to the Notifications and Miscellaneous Settings section and click the drop down arrow at the right hand side expand this section.
2. Specify alert tone settings in the **Alert Tones** section. Refer to the field description information in the following table:

Setting	Description
On/Off Network Alert	**On/Off Network Alert** plays a tone when you are out of the range of the wireless network. The audible warning is a convenient reminder if you are supposed to leave Vocera devices behind when you go home. However, if you routinely move between buildings, and the network does not cover the outdoor spaces, you may not want to hear an alert tone. By default, the **On/Off Network Alert** check box is selected.

Setting	Description
Low Battery Alert	**Low Battery Alert** sounds an alert when the battery needs to be recharged. By default, the **Low Battery Alert** check box is selected.
Text Message Alert	**Text Message Alert** plays a tone when you receive a new text message. The tone sounds only once for each new message. An envelope icon also appears on the Vocera device display to indicate that you have unread text messages. By default, the **Text Message Alert** check box is selected.
Voice Message Alert	**Voice Message Alert** issues a tone when you receive a new voice message. The tone plays only once for each new message. A telephone icon also appears on the Vocera device display when you have not played your voice messages. By default, the **Voice Message Alert** check box is selected.
Disable Alerts in DND Mode	**Disable Alerts in DND Mode** prevents all alert tones when you put the Vocera device in Do Not Disturb mode. By default, the **Disable Alert Tones in DND Mode** check box is not selected.

3. Choose any reminders you want to enable in the **Reminders** section. Refer to the field description information in the following table:

Setting	Description
Text Message Reminder	Select **Text Message Reminder** to play a tone on the Vocera device every 15 minutes until you pick up new text messages. By default, the **Text Message Reminder** check box is not selected.
Voice Message Reminder	Select **Voice Message Reminder** to play a tone on the badge every 15 minutes until you pick up new voice messages. By default, the **Voice Message Reminder** check box is selected.
DND Reminder	Select **DND Reminder** to play a tone on the Vocera device every 15 minutes when the device is in Do Not Disturb mode. By default, the **DND Reminder** check box is selected.

4. Choose any notifications you want to enable in the **Automatic Notifications** section. Automatic notifications allow you to bypass certain operations without confirming them.
   Refer to the field description information in the following table:

Setting	Description
Missed Call Notification	**Missed Call Notification** causes the Genie to notify you of missed calls since the last time you pressed the Call button. The Genie also announces the names of people who left messages. You may prefer to use the "Who called?" command when you are in a quiet area to learn who called. If you prefer using the "Who called?" command, you can clear the **Missed Call Notification** setting. By default, the **Missed Call Notification** check box is selected.
Disable Voice Message Notifications	**Disable Voice Message Notifications** causes the Genie to suppress notifications when you receive a message. However, you may still hear a voice message alert tone (if the Voice Message Alert option is selected), and a telephone icon appears on the Vocera device display if you haven't played the voice messages. By default, the **Disable Voice Message Notifications** check box is not selected.

5. In the **Message Play Settings** section, specify the behavior of the "Play Messages" commands.
   Refer to the field description information in the following table:

Setting	Description
Play Older Messages First	**Play Older Messages 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** check box is not selected.

Setting	Description
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, you 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** check box is selected.
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, you 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** check box is not selected.

6. In the **Call Setup** section, specify the behavior of the call setup.
   Refer to the field description information in the following table:

Setting	Description
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, "Can you talk to [*CallerName*]?" 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** check 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 Vocera device 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 Vocera device, all audio plays through the headset by default. Consequently, if you are not wearing your headsets all the time, you may not hear an incoming announcement, and you may not know that someone is trying to contact you. If you select **Announce Through Speaker**, you can leave your headset plugged in, and simply put them on to communicate after you hear the announcement. If **Announce Through Speaker** is turned on and you are wearing your headset when a call comes in, you may not hear an announcement in a noisy environment (because it plays through the speaker); however, you 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** check box is selected.
Press Button to Accept Call	Select the **Press Button to Accept Call** setting if you want to have a choice to accept or reject incoming calls by pressing the Call or DND/Hold button. This feature is useful in certain high-noise environments. **Note:** Selecting this feature disables the use of "Yes" and "No" voice commands to accept and reject incoming calls. Vocera allows you 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 accept or reject calls prematurely, without listening to user input. To avoid these problems, select this check box to enforce the requirement to answer calls using buttons only. By default, the **Press Button to Accept Call** check box is not selected.
Enable Paging	Select to enable the Vocera Access Anywhere paging capability. By default, the Enable Paging check box is selected.

Status

The **Status** section of the **navigation bar** in the Vocera Platform Web Console allows you to assess the status and health of various system components.

- Audit Log on page 97
- Adapter Services on page 116
- Device Monitor on page 119
- Database Cluster on page 122
- Voice Cluster on page 126
- Queues on page 137

Audit Log

View and manage system event messages on the Vocera Platform in Audit Log.

Auditing provides a means of recording events which indicate problems in the system's setup or stability. Events may also be useful to an administrator or support personnel in determining a sequence of events during processing.

Commonly audited information may be the success or failure of rule processing, incoming messages from a remote system (except responses) that are being processed by an adapter, failures while processing an incoming message, success or failure in connecting to a remote system as well as lost connections, and success or failure when opening and closing the firewall ports.

Vocera Platform treats all audit log event codes as new in an upgrade, and audit log event codes previously turned off may be turned on. Please make a note of all audit log event codes prior to upgrading, as this has a potential impact to clients.

Using Audit Log in the Vocera Platform Web Console, you can search and view audit event messages, and manage the Audit Log configuration settings. Tools are provided in the toolbar to filter the events displayed in Audit Log in order to narrow the focus to an area of interest. Information about the source and quantity of the displayed event logs is available below the Audit Log grid. By default, Audit Log displays the latest audit events in descending time order without any filtering.

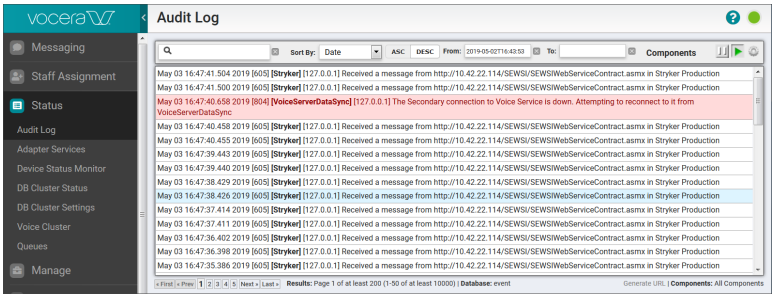
Audit Log data is not stored locally; the display refreshes periodically (every 3 seconds) with the selected results, filtering, or ordering information. Users can pause the refresh in order to view the results on the page; retrieval is automatically paused if the user is viewing a page of results other than the first page.

Navigating to Audit Log

Access the reported system event logs in the Vocera Platform Web Console.

Users with the appropriate login credentials can access the logs generated for auditable events in the Vocera Platform Web Console. See a System Administrator for assistance if needed.

1. Navigate to **Status > Audit Log**.
   The Audit Log displays.
2. View the scrollable list of audit events in Audit Log. Note that audit events with a priority level of Error display in red.



3. Use the details provided in the following table to interpret the data provided for the reported audit events.

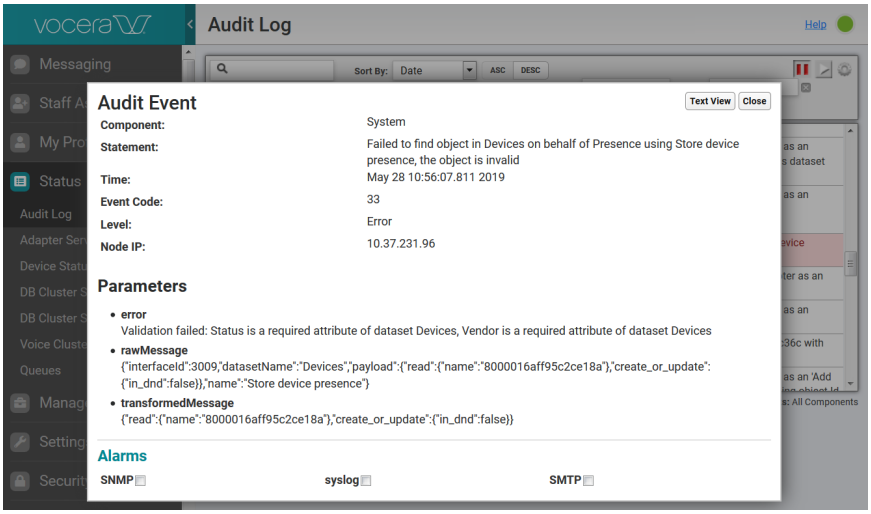
Field	Description
Timestamp	Date and time of the audit event.
Event code	Event code logged for the audit event.
Component	Name of the component logged for the audit event.
Node IP	Address of the server node for the audit event.
Event Statement	Content of the audit event message.

Viewing Audit Event Message Content

Event logs contain valuable auditable information about the system's setup or stability.

The Audit Log page provides the ability to view system event messages. These messages may be confirmation that a process is running correctly, or an indicator that a process has encountered an error. Move the cursor over the Audit Log entries to highlight an audited event of interest.

1. Click an Audit Log entry to access details about that particular entry.
   The Audit Event message dialog displays.
2. View the Audit Event message dialog information about the selected event.



3. Use the information provided in the following table to understand the details provided in an audit event's message.

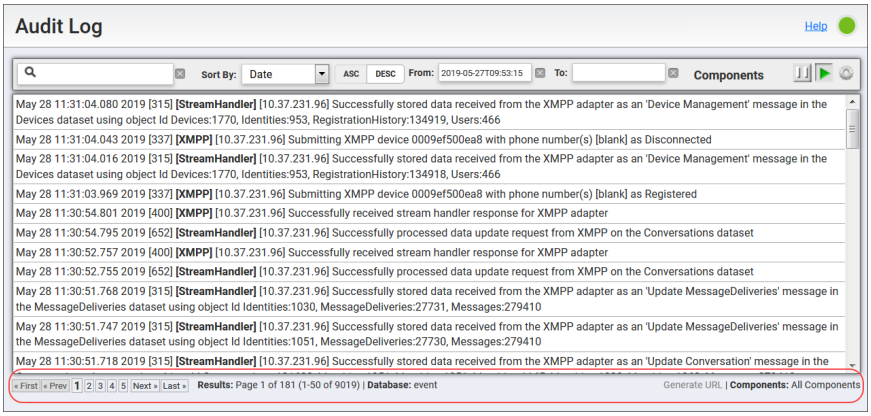
Message Element	Description
Component	The system component that is the source of the Audit Log entry is displayed. Examples of what might be displayed in this field are Audit, System, StreamHandler, IncomingEmail, etc.
Statement	The complete statement that is being recorded in the Audit Log about a particular event is displayed. This statement will vary based on the type of event.
Time	The timestamp that corresponds to the Audit Log event is displayed.
Event Code	The corresponding event code for the Audit Log event that is being viewed is displayed.
Level	The priority level of the event is displayed. Three levels are provided by default: • Level 1 is Info • Level 2 is Warning • Level 3 is Error
Node IP	The Node IP is the IP address of the VM that is hosting the Vocera software.
Parameters	A Parameter is any information that is relevant to the event code, but is not included in the event code statement. The information that appears in the Parameters section can vary from each Audit Log event. Examples of what might be displayed in this field are the raw message of the event, any exceptions to the event code, and any parameters not included in the event code statement.
Alarms	An Alarm tells the system how to notify the user of a particular event. This functionality is the same as when configured in **Notifications**, but in a more streamlined fashion. There are three responses that the system can utilize: a Simple Network Management Protocol (SNMP) alert, record it to the syslog, or send an email via Simple Mail Transfer Protocol (SMTP). Select the checkbox for the appropriate alarm for this particular alarm. When searching events, all of the text on this screen is searched as well. To change the alarm type for future events, change the alarm setup in the **Configuration** section of Audit Log.

4. Select **Text View** in the upper right corner to access a simple version of the details.
5. When you have finished working with the audit event details, select **Close** in the upper right corner to return to the Audit Log list view.

Viewing Audit Log Pagination Results

Page through the audit event list, and see the number of page results, the database being viewed, and the components selected for view. You can also capture the URL of the current database view to share with other users.

1. In Audit Log, view the status information in the footer.



2. Use the details provided in the following table to understand the status information provided in the footer.

Field	Description
Paging Options	Use the provided buttons to access the pages of event logs. Page access options are as follows: First, Previous, numbered pages, Next, Last.
Results	Lists the number of pages of log entries available, and identifies the page currently viewed.
Database	Displays the name of the database currently accessed.
Generate URL	Click Generate URL to copy the URL if you wish to share the configured settings display.
Components	List of components that the user has selected for viewing. By default, all components are viewed.

SMTP Event Notification Email and PHI

Understand that audit settings can be configured to avoid exposing protected health information (PHI) when using email for audit event notifications.

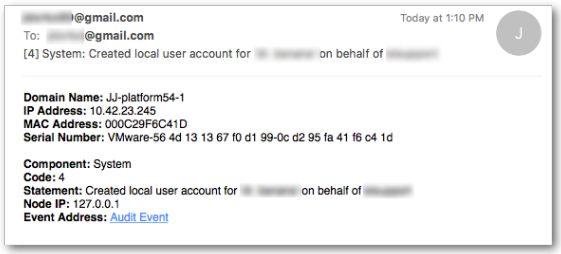
Vocera uses SMTP technology as an alerting tool. When an audit event marked for this type of alert is executed, an email is sent to the personnel who are able to perform corrective actions on the system. To avoid exposing any protected health information (PHI), the audit content is not included in the email but is available via a link; the email recipient can follow the link in the SMTP alert to view the audit event details.

A specified event code triggers the notification email, which is sent to the configured recipient as an HTML document. The email contains the event code, the component which sent the audit event, the statement, and a link to the specific audit event. In addition, the email contains information specific to the Vocera Platform, including the domain name, IP address, and so forth.

To set up email notifications, first configure the SMTP Mail Server settings in the **Destinations** section that will handle the outgoing email notifications from Audit. See Configuring SMTP Settings on page 110 for details.

Then, in the **Notifications** section, select the event codes that will trigger an email notification, and the SMTP destination. See Working with Notifications Settings on page 108 for details.

Once configured, the email notifications that are triggered will contain an **Audit Event** link in the Event Address field as shown below. The email recipient can click the link to access the event details, which potentially contain PHI.



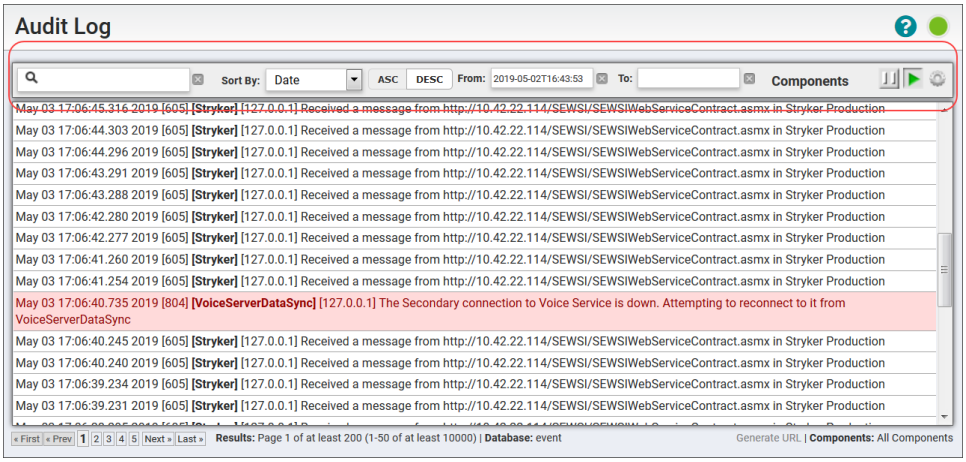
Working with Audit Log Results

The Audit Log toolbar provides multiple functions that allow you to locate and display the results you need in the scrollable list of audit events.

The default display contains a list of current audit events reported in real time. This section contains functionality that allows you to work with the audit event display quickly and effectively.

The top row of the Audit Log section contains tools that provide the ability to search, sort, and filter Audit Log entry results. Below this toolbar, the log entries display in chronological order by default.

The provided tools include a search field, a preconfigured list of elements used to Sort By, and an Ascending and Descending sort toggle option. The toolbar also includes a Date Range option to filter results into a chosen timeframe, a field for sorting by Component name, as well as the ability to control the active display with a Pause and Play option.



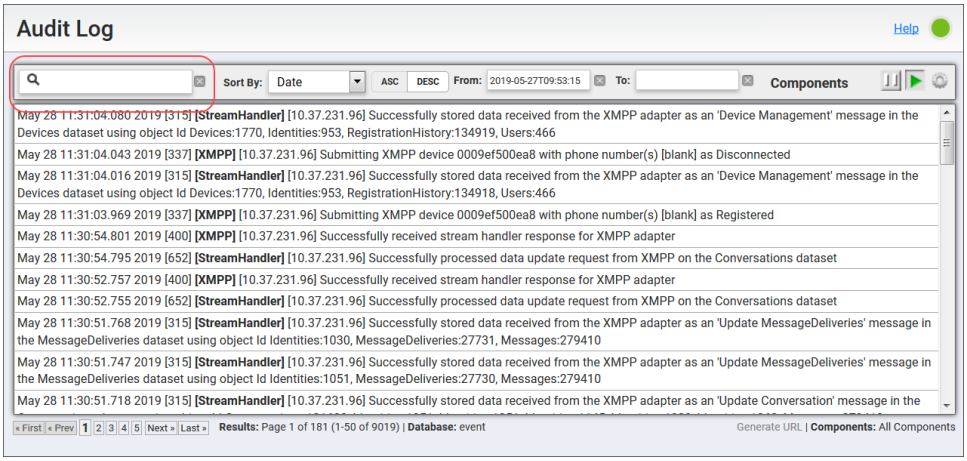
Searching Audit Log Events

The Search field provides the ability to search the Audit Log entries, utilizing Postgres full text searching against the following audit event table columns: Statement, Event Code, Parameters, Node IP.

The following parameters apply to the search functionality:

- Text search is case insensitive, and the order of multiple search terms is not considered.
- Prefixes are included in both alphabetic and numeric search. Suffixes are not included in any search.
- Punctuation and special characters are ignored in searches. When a special character is surrounded by characters in a word, then the special character will split the word because it is ignored by the search engine.

1. Enter the search term in the Search field.



The Audit Log entries in the scrollable list are restricted to display only entries that match the search criteria.

2. Utilize the following examples to work with the Audit Log search capability.

Condition	Search String	Result Examples
Text Case	error log	error log, log error, Error Log
Numeric Order	36	36, 366, 36xx
Alpha Order	error log	error log, log error, error, log
Numeric Prefix	36	36, 366, 36xx
Alpha Prefix	Rsynch	Rsynch3, rsynchxxx
Alpha Suffix	failed	fail, failed
Special Characters	to night	To*night (string will break at the special character), to night
Special Characters (including punctuation)	$, ?, &	(no results returned)

3. Clear the Search field, and all entries are displayed in the Audit Log event list.

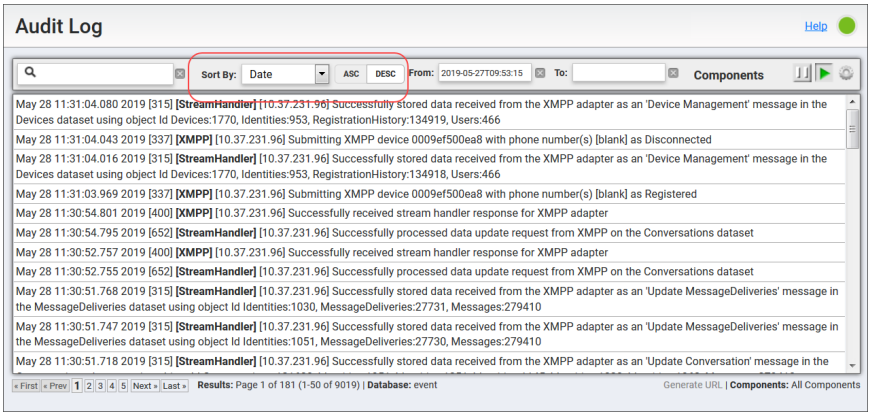
Sorting Audit Log Events

The Audit Log page contains a Sort By filter and an Ascending/Descending display option in the toolbar to allow you to quickly view the information you want.

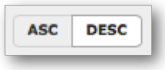
1. Select an item in the **Sort By** drop-down menu to sort the displayed Audit Log entries by a reported detail. By default, results are sorted by **Date**.

   The following options are available to narrow the list of displayed entries:

   - Component
   - Date
   - Event Code
   - Level
   - Statement
   - Node



2. Select the corresponding button to sort the entries in **Ascending** or **Descending** order. By default, results are sorted in **Descending** order.

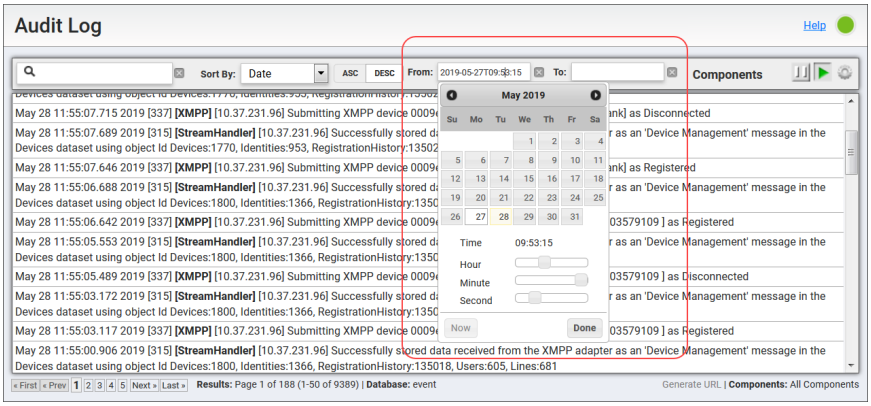


Filtering Audit Log Events by Date Range

A date range filter can be applied to the Audit Log entries to display only the entries logged within a specified date range.

The Audit Log entries automatically filter and display based on the range entered. The search can be filtered further by selecting a time frame within the date range. Use of these features will allow a more focused search result within the specified date range.

1. Place the cursor within the field labeled **Fom:** to select a date range.
   The calendar drop-down utility displays.
2. Select the date from the calendar on which you want your date range filter to begin.



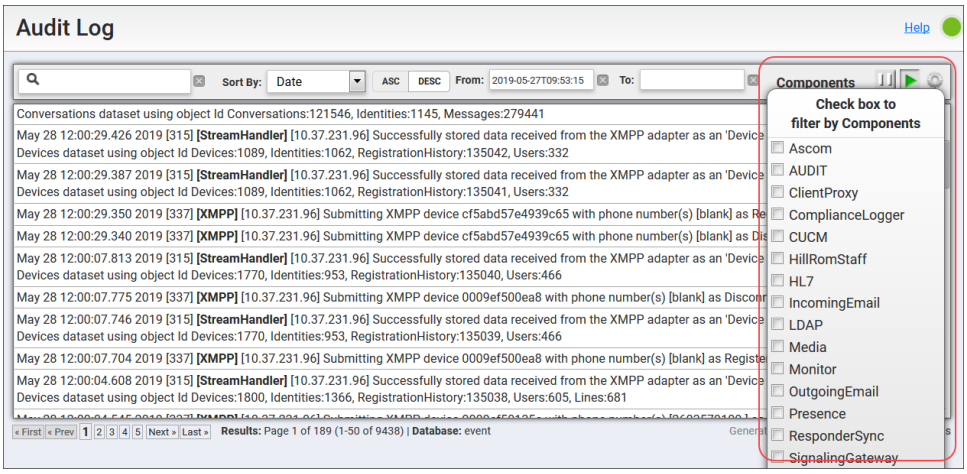
3. To further refine the results of the search, use the slide bars to the right of Hour, Minute, and Second. These bars can be used alone or in combination with one another.
4. Place the mouse within the date range field labeled **To:** and repeat the calendar actions to complete the date range.
5. Clear the date range fields after filtering, and all entries are displayed again.

Filtering Audit Log Events by Component

Audit Log entries can be filtered by the system component to which they correspond.

Only components which have made entries in the database currently being viewed will appear in the Components menu.

1. Hold the cursor over **Components** in the toolbar.
   The **Check box to filter by Components** drop-down menu displays.
2. Select the system component, or components, for which you want to view Audit Log entries.



   The Audit Log entries are automatically filtered to show entries related to the component, or components, selected.
3. To view all Audit Log entries after filtering by a component, deselect all selected components from the drop-down menu and all entries are displayed.

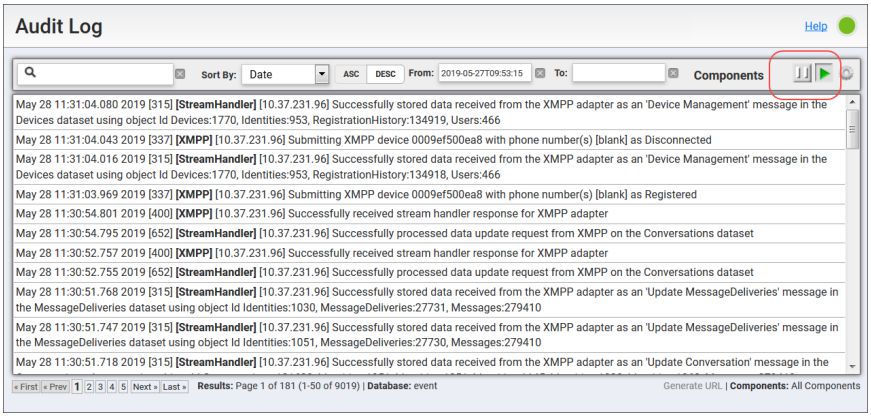
Pausing and Playing Audit Log Results

The Audit Log populates information in real time and you may find it useful to pause the scrollable list to take a closer look at the events.

When the Pause option is selected, the Audit Log stops updating on the user's monitor. The Audit Log is still capturing information in the background and will populate into the user's view of the Audit Log when the Play option is selected.

In addition, retrieval is automatically paused if the user is viewing a page of results other than the first page.

1. Locate the Pause and Play options in the Audit Log toolbar.



2. Select **Pause**.

The Audit Log view on your local machine stops updating.

3. Select **Play**.

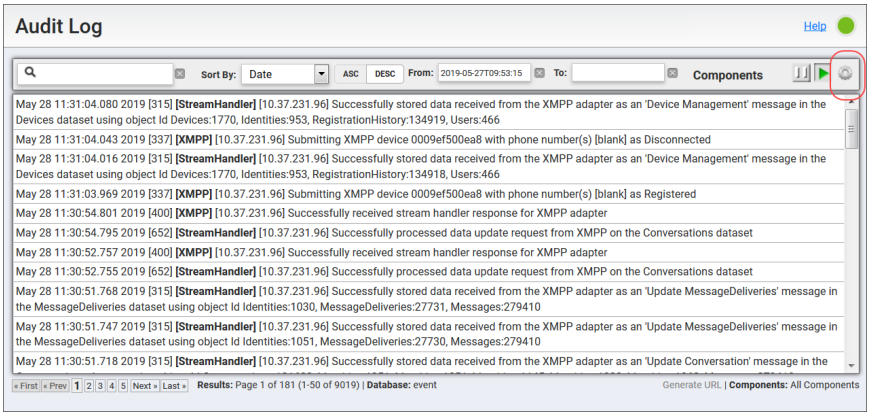
The Audit Log populates with the real time display of events.

Accessing the Audit Log Configuration Settings

The Audit Log configuration settings provide the ability to specify general settings, perform certain database functions, manage Audit Log notifications, and set up delivery options for audit events.

In the Vocera Platform Web Console, navigate to **Status** > **Audit Log** to display the list of audit log entries and the toolbar. For instructions on using the toolbar, see Working with Audit Log Results on page 101.

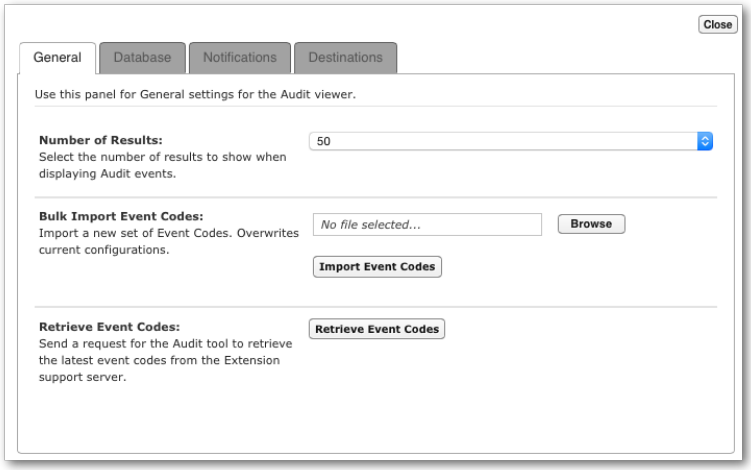
Select the **Gear** option on the Audit Log toolbar to access the configuration settings.



Working with General Settings

The Audit Log's General settings tab allows you to configure the number of results to display, upload a list of event codes into the system, or request the latest event codes.

1. Navigate to the Audit Log configuration dialog as described in Accessing the Audit Log Configuration Settings on page 105.



2. Select a value from the **Number of Results** drop-down menu. You can select to display as few as 10 results or up to 1000 results in the Audit Log display.
   The Audit Log section limits the number of logs displayed in the current view to the selected number.
3. Browse to a list or set of event codes to be incorporated into the system in **Bulk Import Event Codes**, and then click **Import Event Codes**.

   Warning: This operation will overwrite the current configuration. Contact Vocera Support if you have questions about this feature.
4. Select **Retrieve Event Codes** to submit a request to download the latest event codes from the Vocera Support Server.
5. Select **Close** to exit the configuration dialog.
   The Audit Log section displays.

Working with Database Settings

The Audit Log's Database settings tab allows you to view the current database, download the current database (in zip or CSV format), and upload or delete a database snapshot.

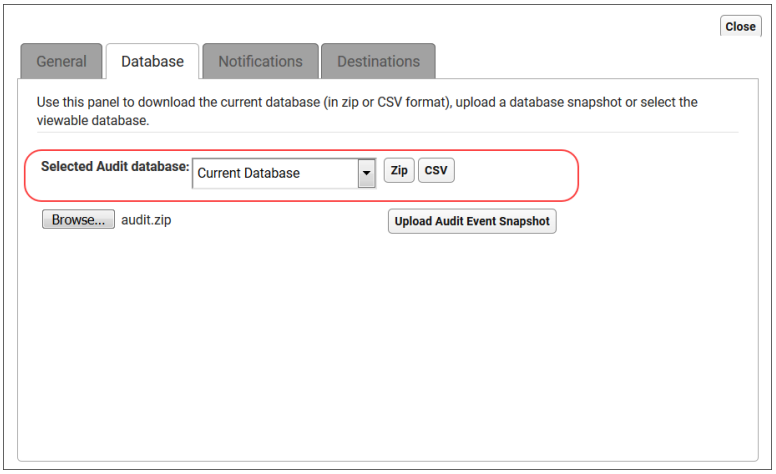
Audit uses a number of partitions (14 by default) to capture audit events over time. The number of partitions has a lower bound of two but no upper bound. A partition is a Postgres table containing audit events within a time bound. The partition's time bound is configurable (24 hours by default) with the minimum number being one hour.

When the system is writing to the last partition, the oldest partition is dropped and a new one partition is created. This partition rotation is not a persistent archive, but provides access to history without the database growing unbounded. Please use the Backups functionality to manage audit event history through regular database backups in the Vocera Platform Web Console.

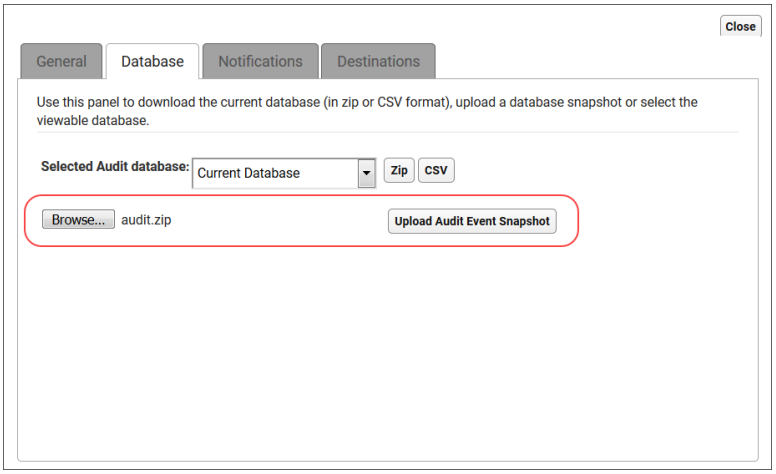
This Database section provides the ability to download the current database in a .zip or .cvs file. The download file may contain all entries across all partitions in the audit log database. Any filter criteria used in the audit log viewer when the snapshot is taken are applied to the downloaded entries. For example, if the audit log viewer is filtered to only show a subset of the audit entries, then the downloaded database snapshot will contain only the entries shown in the audit log viewer.

Warning: The Database will NOT download and restore if the user is utilizing a Mac with the OS X operating system. To work around this issue, disable Safari's automatic archive unzip function: select Preferences > General, and uncheck the "Open safe files after downloading" option.

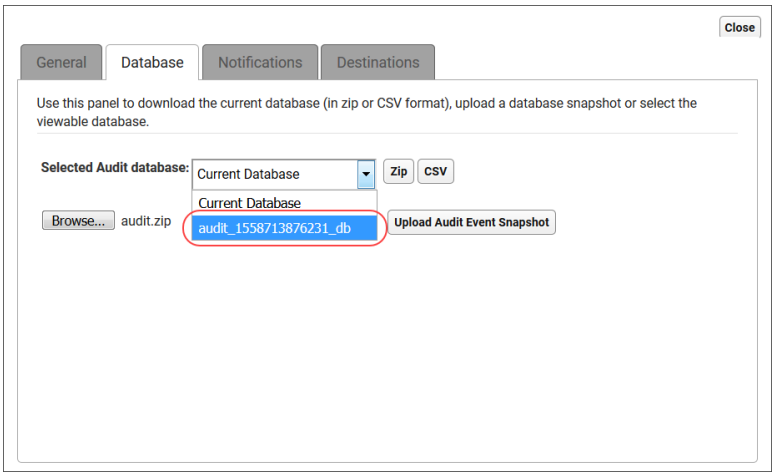
1. Navigate to the Audit Log configuration dialog as described in Accessing the Audit Log Configuration Settings on page 105.
2. In the Database section, select **Zip** or **CSV** to take a snapshot of the current database.



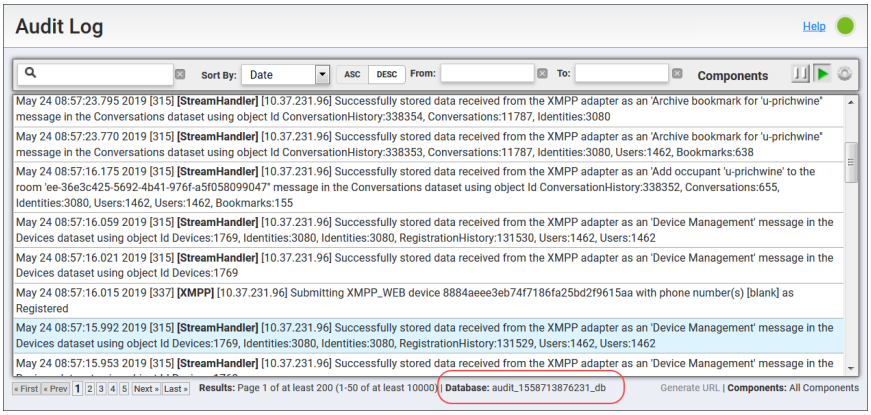
3. Once a snapshot is downloaded to storage, select **Choose File** to navigate to the database snapshot and then click **Upload Audit Event Snapshot** to upload the snapshot to the system.



4. Select the uploaded database snapshot in the **Selected Audit database** field, then click **Upload Audit Event Snapshot** to load it to the Audit Log.

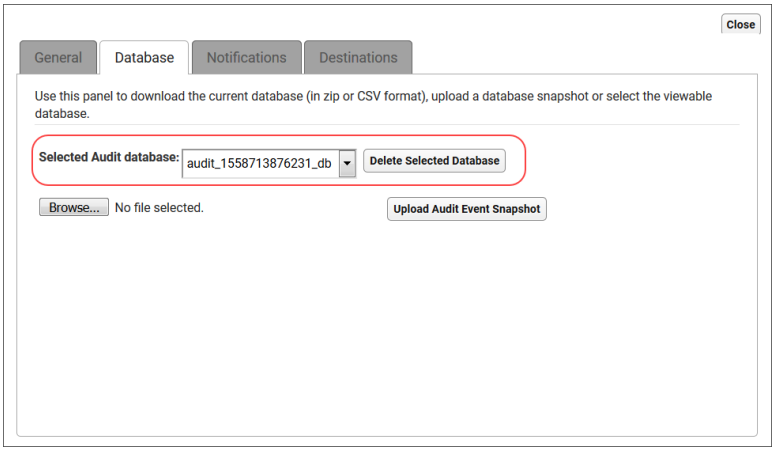


5. Verify the correct snapshot version uploaded by checking the **Database** field in the footer of the Audit Log viewer. Any filter criteria used in the audit log viewer when the snapshot was taken will display in the uploaded entries.



6. To delete a database snapshot, select a database snapshot in the **Selected Audit database** field, then click **Delete Selected Database**.

   The Delete option is provided for snapshots, and is not available when Current Database is selected.



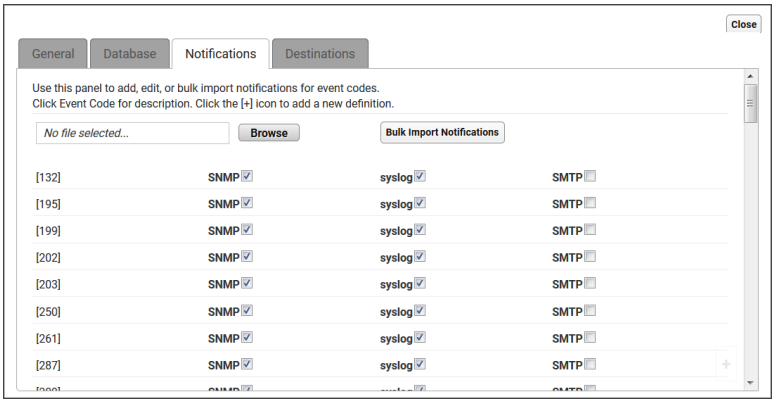
7. Select **Close** to exit the configuration dialog.
   The Audit Log section displays.

Working with Notifications Settings

The Audit Log's Notifications settings allow you to manage the SNMP, Syslog, or SMTP method of sending notifications for an event code, and to bulk import notifications for event codes.

When a notification is configured for an event code, an SNMP trap is sent if SNMP is selected, an e-mail is sent if SMTP is selected, and a syslog event is logged if Syslog is selected.

1. Navigate to the Audit Log configuration dialog as described in Accessing the Audit Log Configuration Settings on page 105.
2. Select one or more of the three delivery methods for each Audit Log event code that should provide a notification; SNMP, Syslog, SMTP.



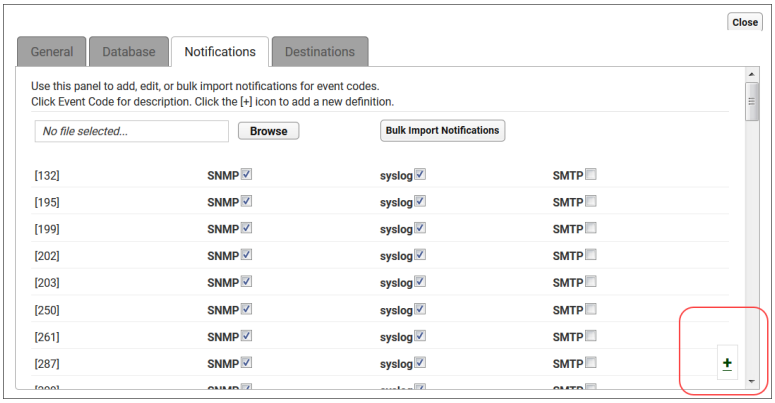
3. To bulk import notifications, browse to and select the file containing the notifications you wish to upload, and then select **Bulk Import Notifications**.

   Warning: This operation will overwrite all saved definitions. Contact Vocera Support if you have questions about this feature.

   The format of the file must be similar to the example below. Use a line for each type (smtp, snmp, syslog) followed by a comma-separated list of events that should be turned on for that service.

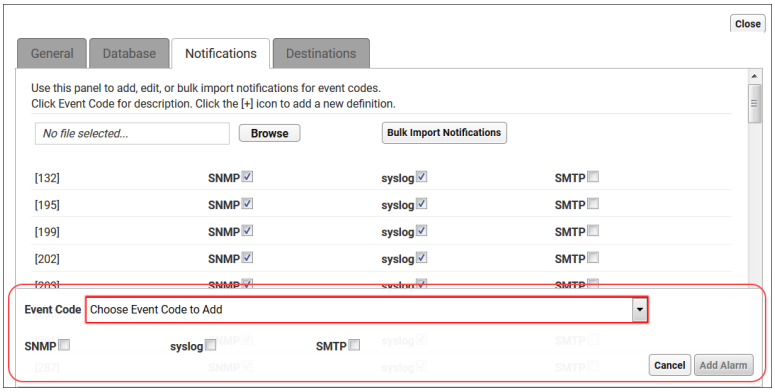
```
smtp,267,268,269,270,271,272,284,296,346,373,376,383,384,409,412,416
syslog,10,11,13,14,16,19,21,23,26,27,31,32,33,43,44,55,56,57,58,85,116,117
snmp,31,260,261,267,268,269,270,271,272,284,285,286,288,294,296,305,312
```

4. To add a new notification, click the + button in the lower right corner of the Notifications section.



A dialog displays.

5. Choose an audit event in the **Event Code** dropdown list, and select the SNMP, Syslog, or SMTP destination for the audit event.



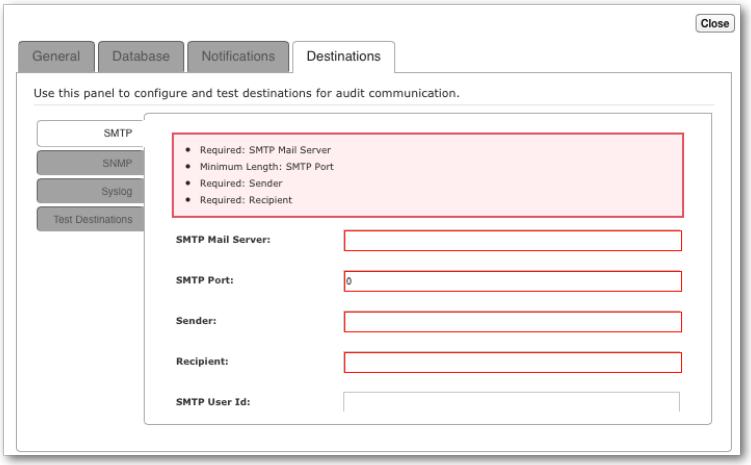
6. Select one of the following options to exit the new notification dialog.
   - Select **Add Alarm** to add the notification to Audit Log.
   - Select **Cancel** to close the dialog with making a change.
7. Select **Close** to exit the Notifications configuration dialog.
   The Audit Log section displays.

Working with Destinations Settings

The Audit Log's Destinations settings allows you to manage the settings for the three delivery options available for every Audit Log event code: SMTP, SNMP, Syslog.

The delivery options that the system can utilize are: send a Simple Network Management Protocol (SNMP) alert, record it to the Syslog, or send an email via Simple Mail Transfer Protocol (SMTP).

In the Destinations section, there are four additional tabs displayed on the left side of the dialog. These provide optional settings to allow a user to input the required information for each of the delivery methods (SMTP, SNMP, Syslog) and a final tab that will allow a user to test delivery in the new configurations.

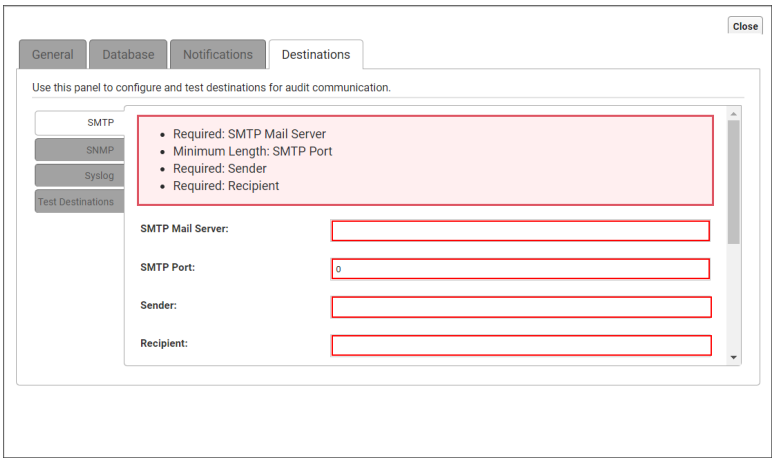


Configuring SMTP Settings

Specific audit event codes can be configured to send an email notification when it is utilized.

Simple Mail Transfer Protocol (SMTP) is an Internet standard for e-mail transmission across Internet Protocol (IP) networks.

1. Select **SMTP** in the Destinations section navigation.



   The configuration fields display.

2. Supply the following required information in the SMTP section to enable email notifications.

   Optional configuration fields in the SMTP section may or may not be utilized by your facility, and are not described below.

Required Setting	Description
SMTP Mail Server	An e-mail client needs to know the IP address of its initial SMTP server and this has to be given as part of its configuration (usually given as a DNS name). This server will deliver outgoing messages on behalf of the user.
SMTP Port	The facility administrators choose whether to use TCP port 25 (SMTP) or port 587 (Submission) for relaying outbound mail to an initial mail server.

Required Setting	Description
Sender	The Sender is the email address that the facility administrators set up from which the email comes. For example, a facility may set up Alerts with an email address of `Alerts@facility.com`.
Recipient	The Recipient is the email address that the Audit Log event codes should be sent to. This is most typically an IT person, or group of IT personnel, within the facility.

3. Select one of the following options once the required fields have been filled out.
   - Select **Save SMTP Configuration** at the bottom of the screen to enable sending an email.
   - Select **Reset Values** to clear the fields without saving any configuration details.
   - In order to test the SMTP configuration, select **Test Destinations** in the left navigation tabs.

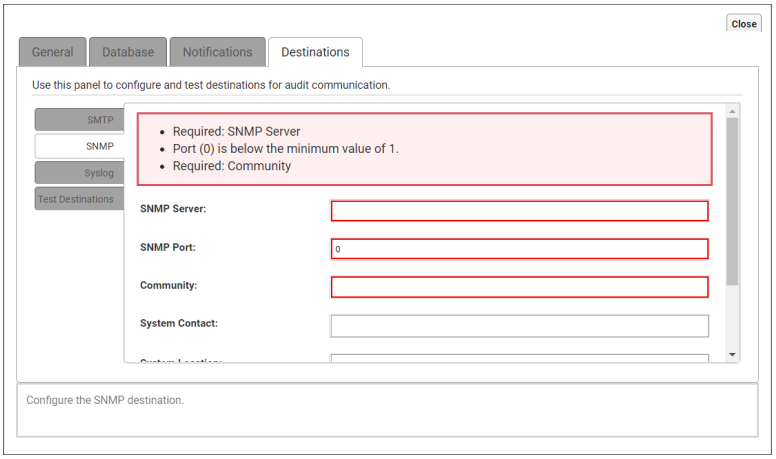
Configuring SNMP Settings

SNMP devices monitor system health and can be used to send messages when configured thresholds are exceeded.

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. An SNMP device listens to monitor the health and well being of various systems around a facility.

In a Vocera Platform implementation, an SNMP device is attached to the physical or virtual server and receives messages when certain thresholds are crossed. The SNMP device is constantly listening for these messages and when one is delivered, the facility is notified via an SNMP Monitoring Tool. This Monitoring Tool is configured by the facility's IT Department to notify the appropriate individuals when a message is received.

1. Select **SNMP** in the Destinations section navigation.



   The configuration fields display.
2. Supply the following information in the SNMP section to enable sending a message.

   Optional configuration fields in the SNMP section may or may not be utilized by your facility, and are not described below.

Required Setting	Description
SNMP Server	This field contains the IP Address or the FQDN within the DNS of the facility's Monitoring Tool.
SNMP Port	This field contains the Port number where the Monitoring Tool is located, usually 162.

Required Setting	Description
Community	This field contains the password that is utilized by the SNMP Monitoring Tool. This must match for traps to be received by the Monitoring tool.

3. Click **Download MIB** at the bottom of the Destinations section. After the download has completed, upload this file to the facility's Monitoring Tool.

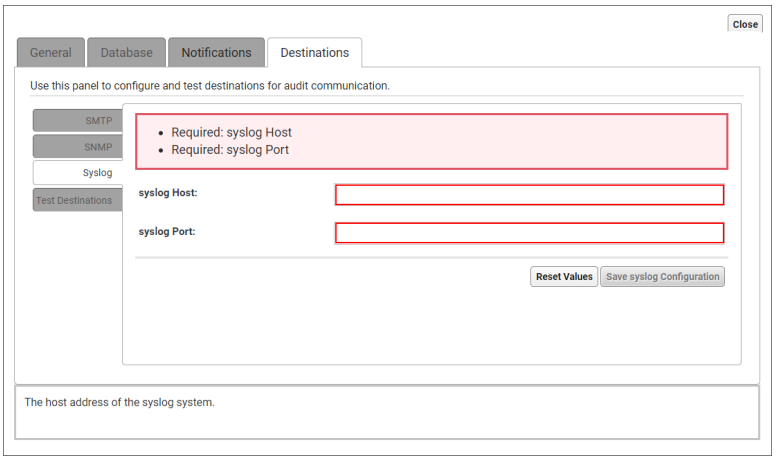
   The MIB file contains information that Vocera exposes to the Monitoring Tool, essentially telling the Montoring Tool what is available to monitor. The MIB file contains all of the Object ID's (OID) of the information that Vocera exposes for monitoring.
4. Select one of the following options when the upload has successfully completed.
   - Click **Save SNMP Configuration** to save the changes.
   - Select **Reset Values** to clear the fields without saving any configuration details.
   - In order to test the SNMP configuration, select **Test Destinations** in the left navigation tabs.

Configuring Syslog Settings

Audit log events can be written directly to the facility's system.

Syslog is a standard for logging system messages. By utilizing the Syslog feature in Vocera Platform, a facility can choose to have Audit Log events written directly into their own Syslog.

1. Select **Syslog** in the Destinations section navigation.



   The configuration fields display.
2. Supply the following information in the Syslog section to enable writing to your system.

Required Setting	Description
syslog Host	This field contains the IP address or DNS name of the device where the syslog is located.
syslog Port	This field contains the Port number of the device where the syslog is located, usually 514.

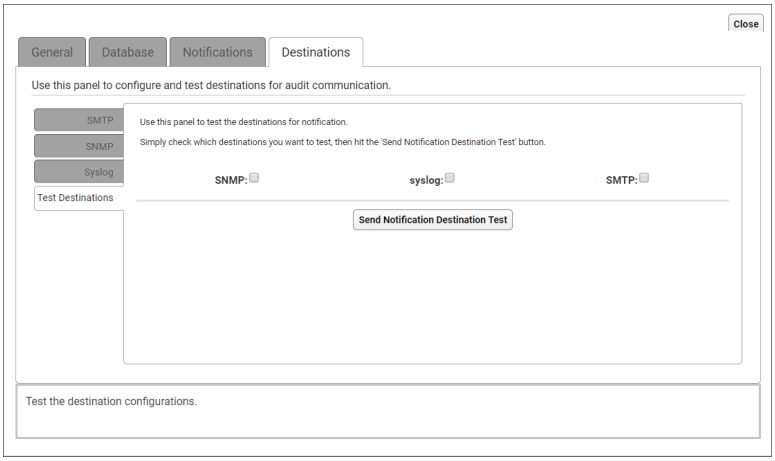
3. Select one of the following options once the required fields have been filled out.
   - Click **Save syslog Configuration** at the bottom of the screen to save your changes.
   - Select **Reset Values** to clear the fields without saving any configuration details.
   - In order to test the syslog configuration, select **Test Destinations** in the left navigation tabs.

Configuring Test Destinations Settings

The Test Destinations section allows a user to test any notification configurations created in Audit Log.

After configuring event code notification in the Destinations section, the Test Destinations dialog allows you to check that the configurations perform as expected.

1. Select **Test Destinations** in the Destinations section navigation.



   The configuration fields display.
2. Check either **SNMP**, **Syslog**, **SMTP**, or a combination of those boxes. After the appropriate check boxes have been selected, click **Send Notification Destination Test**.
3. If the test messages reach the intended recipients appropriately, there is nothing further to do. If the test messages do not reach the intended recipients, then make the adjustments in the appropriate destination section: SMTP, SNMP, or Syslog.

Filtering Audit Events for Vocera Analytics

Filter Data Export related events from going into the Audit database, and write them to the Audit debug log instead, to reduce the volume of logging in Audit.

After installing Vocera Data Export Adapter rules for Vocera Analytics, the volume of Audit events increases dramatically. This increase in the volume of Audit events at a medium or large facility may cause the Audit database to be unusable and increase the risk of performance issues.

Filters are stored in the configuration property files used by Audit. Filters can also be used to filter other Audit events, not just those related to Vocera Analytics.

Note: The default filter configuration should be sufficient to filter out the large volume of events generated by Vocera Data Export Adapter rules.

When Audit events arrive at the Event Manager in the Audit process, the Event Manager will determine if the event matches any filter and write it to the debug log instead of storing it or sending notifications. If the event matches a filter, the event will be written to the debug log at INFO level in its raw JSON form prepended with `Filtered`.

Using Audit Properties to Filter Events to Debug Log

Filters are specified in the Audit property configuration files.

The default filters are specified in the default properties file, found at /opt/EXTENSION/conf/audit/audit.properties.

Important: Do not edit the /opt/EXTENSION/conf/audit/audit.properties file.

You can add to or replace the default filters by creating a **.user** properties file at /opt/EXTENSION/conf/audit/audit.user.properties.

The default filters are:

```
filter.01=interfaceRefName~/Data\\s*Export/
filter.02=component~/^DataExport$/
filter.03=rawMessage~/\\bSignalingPretimeoutNotification\\b/
filter.04=rawMessage~/\\bWakeupNotification\\b/
```

To override the filters without replacing them, place the following in /opt/EXTENSION/conf/audit/audit.user.properties:

```
filter.01=
filter.02=
filter.03=
filter.04=
```

To change the existing filters, specify new values for the same filters.

To add a filter, use a new filter name such as "filter.05".

Filters are specified using one or more conditions. Conditions are composed of the Audit field/property and a regular expression that the field/property must match. They are formatted in the property file as follows:

```
filter.<number>=<audit field or property>/<regular expression>/,<audit field or property>/<regular expression>/,...
```

Where:

- <number> is a value to uniquely identify the filter.
- <audit field or property> is an Audit field such as code, component, or an Audit property as defined in the property database.
- <regular expression> is a regular expression to match the field/property.

Use a comma or space (or anything that doesn't look like a condition) to separate multiple conditions.

A filter matches an Audit event if all conditions match. The regular expression can match anywhere in the value. To match the complete value, use anchors in the regular expression; for example, /DataExport/ will match MyDataExport, but /^DataExport$/ will not.

Filters will never match warning or error level Audit events. Filtering only applies to INFO level events.

Important: Filters that do not match the above pattern will be ignored and logged as errors to EIAudit.log.

Filters can be tested by viewing /opt/EXTENSION/log/EIAudit.log. All filtered Audit events are logged as INFO log entries starting with {{Filtered :}} followed by the JSON for the Audit event.

Important: Use two of the backward slash (\\) because /opt/EXTENSION/log/EIAudit.log is a Java properties file. Matching a forward slash (/) is not supported in the filter, because the forward slash is used to mark the beginning and end of a regular expression.

Enabling and Disabling Filtering

All filters may be disabled to facilitate troubleshooting. You can reload filters from the property configuration files to enable filtering again.

The default filters will eliminate most Data Export audit events from the Audit database. You can disable a default filter if you wish to troubleshoot Data Export issues, for example, and reload the filter when finished troubleshooting.

1. To disable filtering, enter the following URL in your browser:

   ```
   http://extension.hospital.com/osgi/audit/setApplyFilters/false
   ```

   You should see the following result:

   ```
   {"results":"success"}
   ```
2. To reload filters from the property configuration files and enable filtering, enter the following URL in your browser:

   ```
   http://extension.hospital.com/osgi/audit/setApplyFilters/true
   ```

   You should see the following result:

   ```
   {"results":"success"}
   ```

Adapter Services

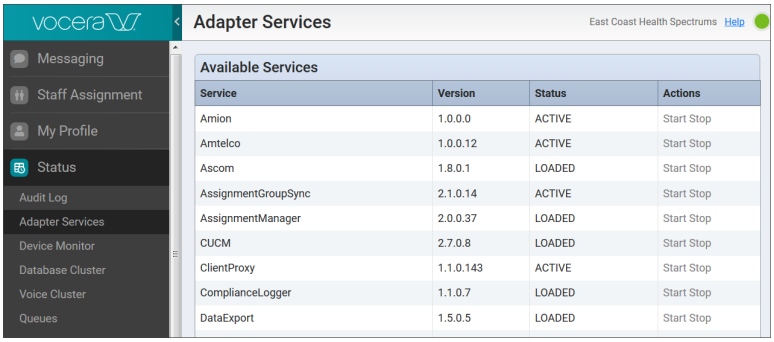
The Vocera Platform Web Console provides the ability to manage and monitor the service status of adapters installed on the Vocera Platform.

Adapters can send information to and receive information from the Vocera Platform, as well as monitor and collect data. On the Adapter Services page, you can verify that an adapter is installed on the Vocera Platform, check the current version of an adapter, verify an adapter's service status, and start or stop an adapter service.

In order to be utilized by Vocera Platform, an adapter component is first installed and configured, including selecting the Enabled setting, and finally the adapter's service is started. The service must be running for the Vocera Platform to implement the functionality designed in the adapter. See Vocera Adapters for details about installing and configuring a specific adapter.

For information about accessing and working with the adapters installed on your system, see Adapters on page 298.

To monitor an adapter's service, navigate to **Status > Adapter Services** in the Vocera Platform Web Console.



Monitoring Adapter Services

The Adapter Services page displays the installed adapters by name, version, activity status, and provides an option to start or stop the adapter's service.

An adapter service must be running in order for the Vocera Platform to utilize the adapter's functionality.

Click Stop or Start to manage an adapter's service. The Adapter Services page updates dynamically, displaying STOPPING or STARTING in the Status field until a status of ACTIVE or NOT_ACTIVE is reached, depending on the action undertaken. For an example using the Adapter Services, see Starting and Stopping Adapter Services on page 117.

Understand the information displayed in the Adapter Services page using the table below.

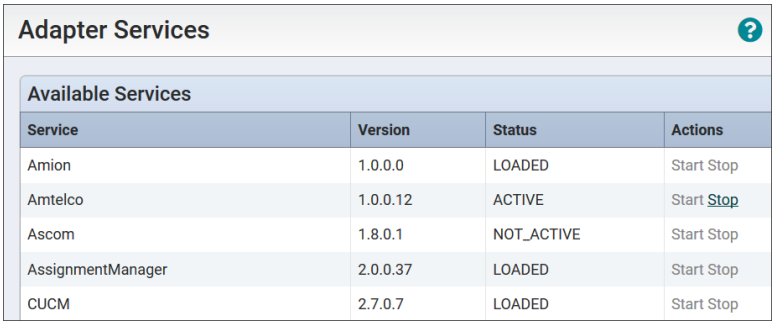
Fields	Description
Service	Displays the installed adapter's reference name.
Version	Displays the currently installed version of the adapter.
Status	Displays the adapter's current service status on the Vocera Platform. Status will display one of the following regarding the adapter's service on the system: • IN ERROR—problem loading the adapter • LOADED—adapter is loaded, not activated • ACTIVE—adapter is loaded and running • NOT_ACTIVE—adapter is loaded, not currently running
Actions	Click Stop or Start to manage the adapter's service. Stop and Start actions apply under the following conditions: • When the adapter is running, Stop can be implemented (Start is not an option). • When the adapter is not running, Start can be implemented (Stop is not an option). • When the adapter's status is LOADED, NOT ACTIVE, or IN ERROR, then Start can be implemented (Stop is not an option).

Starting and Stopping Adapter Services

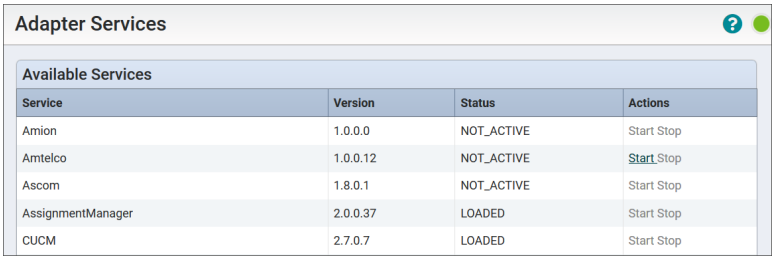
The Adapter Services page provides the ability to start and stop an adapter service on the Vocera Platform.

Navigate to **Status > Adapter Services** in the Vocera Platform Web Console to start or stop an installed adapter. For an explanation of the service status values and the actions that are allowed per status, see Monitoring Adapter Services on page 116.

1. Select an adapter in the **Adapter Services** page.
2. Select **Start** or **Stop** in the Actions column. In this example, click Stop to stop the Amtelco service.



3. Verify that the status changes to **NOT_ACTIVE**, indicating the adapter service is no longer running on the Vocera Platform. In this example, the Amtelco service now displays Not_Active status.



In the Actions column, the Start option is now available and the Stop option is not available.

4. Toggle start and stop actions as needed for the selected adapter, or select another adapter service to manage.

Device Monitor

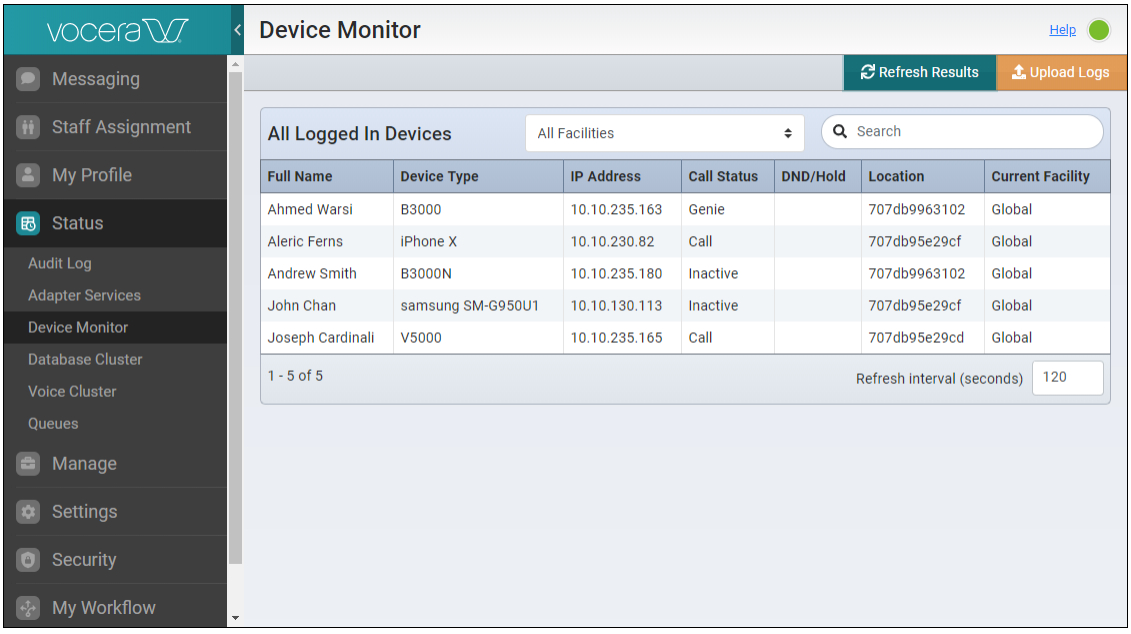
View and monitor the status of devices and users logged into your system.

You can use the **Device Monitor** in Vocera Platform Web Console to periodically monitor the status of devices and other useful information.

The **Refresh Results** button on the top left hand corner of the **Device Monitor** page allows you to refresh the information displayed in the All Logged In Devices section. If you prefer to set an automatic page refresh, you can use the **Refresh Interval** field at the bottom of the **Device Monitor** page to set a refresh time interval (in seconds). You can also use the **Upload Logs** button on the top left hand corner of the **Device Monitor** page to upload device diagnostic data to the system. For more information on tasks you can perform from the Device Monitor page, see Working With Device Monitor on page 120.

System administrators, system device managers, and system group managers can utilize the Device Monitor functions to monitor and manage devices. See Device Management Roles to learn more about these roles.

To view all logged in devices in your system, select **Device Monitor** in the **Status** section of the navigation bar. The Device Monitor page displays with a list of devices and related information.



You can view the following information about all logged in devices and users:

Field	Description
Full Name	Displays the names of all users who are currently logged in.
Device Type	Displays the type of device the user is currently using.
IP Address	Displays the network address of the device. 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	Displays the call status. If the user is in an active call, `call` status is displayed. If the device is idle, an `inactive` status is displayed. If the user is doing any activity that requires the Genie, such as saying a voice command, listening to message, or recording a name or greeting, the Call Status displays `Genie`. Call Status 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	Displays `DND` if the user has put the device in Do Not Disturb mode, or `Hold` if the user has placed a call on hold. Otherwise, this field is blank.
Location	Displays 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 Facility	Displays the name of the facility where the user is currently logged in.

Working With Device Monitor

Use the **Device Monitor** in the Web Console to monitor device status and activities.

The Vocera Platform Voice Service updates **Device Monitor** according to the number of seconds you set as the refresh interval.

You can use the **Device Monitor** to perform the following tasks:

- Refresh and update the display immediately — click **Refresh Results**.
- Specify a different time between automatic updates — enter a value between 5 and 3600 seconds in the **Refresh Interval** field, and click **Refresh Results**. The default value is 120 seconds.
- Sort users by all columns (Full Name, Device Type, IP Address, Call Status, DND/Hold, Location, or Current Facility) — click the corresponding column heading to sort accordingly. The default setting for the display shows user names sorted alphabetically with the **Full Name** displayed first.
- Return to alphabetical sorting — click the **Full Name** column heading.
- View a list of users logged-in at a specific facility — choose a facility from the **Facility** filter list.
- Search for a specific user — enter the last name or part of the last name in the **Search** field, then press the Return key on your keyboard.

In addition to the above mentioned tasks, you can use **Device Monitor** to upload Vocera device logs. See Uploading Device Logs for more information.

Uploading Device Logs

Conveniently upload the device diagnostic data for one or more selected Vocera devices.

Using the configuration menu on your Vocera device to upload logs is a bit tedious. You can use the upload logs function in the Web Console to upload the device diagnostic data.

When you upload the badge logs (B3000, B3000n, or V5000), the files are assembled into a single `.tar.gz` file in the uploads `/opt/vocera/logs/badgelogcollector/uploads` directory on the Vocera Voice Server. The format of the file name is `DATETIME-USERNAME-BADGEMAC-udd.tar.gz`.

Similarly, you can upload logs for smartphones using the Vocera Vina application. When you select an Android or iOS phone in the **Device Monitor** and click **Upload Logs**, the logs are assembled into a `-android.zip` or `-ios.zip` file and uploaded in the `/opt/vocera/client-log` directory.

The log file name format is `USERNAME-DATETIME-`*ios/android*`.zip`.

1. Select **Device Monitor** in the **Status** section of the navigation bar.
   The Device Monitor page displays with a list of devices.
2. Select one or more devices and click **Upload Logs**.
   Depending on the device you selected, you may hear the following message from Genie: "Uploading badge diagnostics data, please wait." Once the logs are updated, Genie says, "badge diagnostic upload complete."

Note: The default refresh timer is paused when one or more devices are selected. When no devices are selected, the timer resumes. You can click **Refresh Results** to clear all the selected devices and refresh the screen.

Database Cluster

View and monitor the state of each node and the status of the Core, Audit, and Message Bus databases through Vocera Platform Web Console.

Viewing and monitoring the database cluster status allows you to ensure that the database on a node is always in sync. The **Database Cluster** section in the Web Console provides a Repair option if a database on a node is out of sync You can also enable or disable nodes from the **Database Cluster** section.

Your system administrator must set up the system via the **Network Settings** in the **Settings** section of the Vocera Platform Web Console before setting up database clustering. A node can only be added to a cluster if it has a static IP address, see Editing Network Settings on page 325 for more information. Once the database clusters are configured, you can use the Web Console to manage, restart, and monitor the status of the database clusters.

Viewing Database Cluster Status

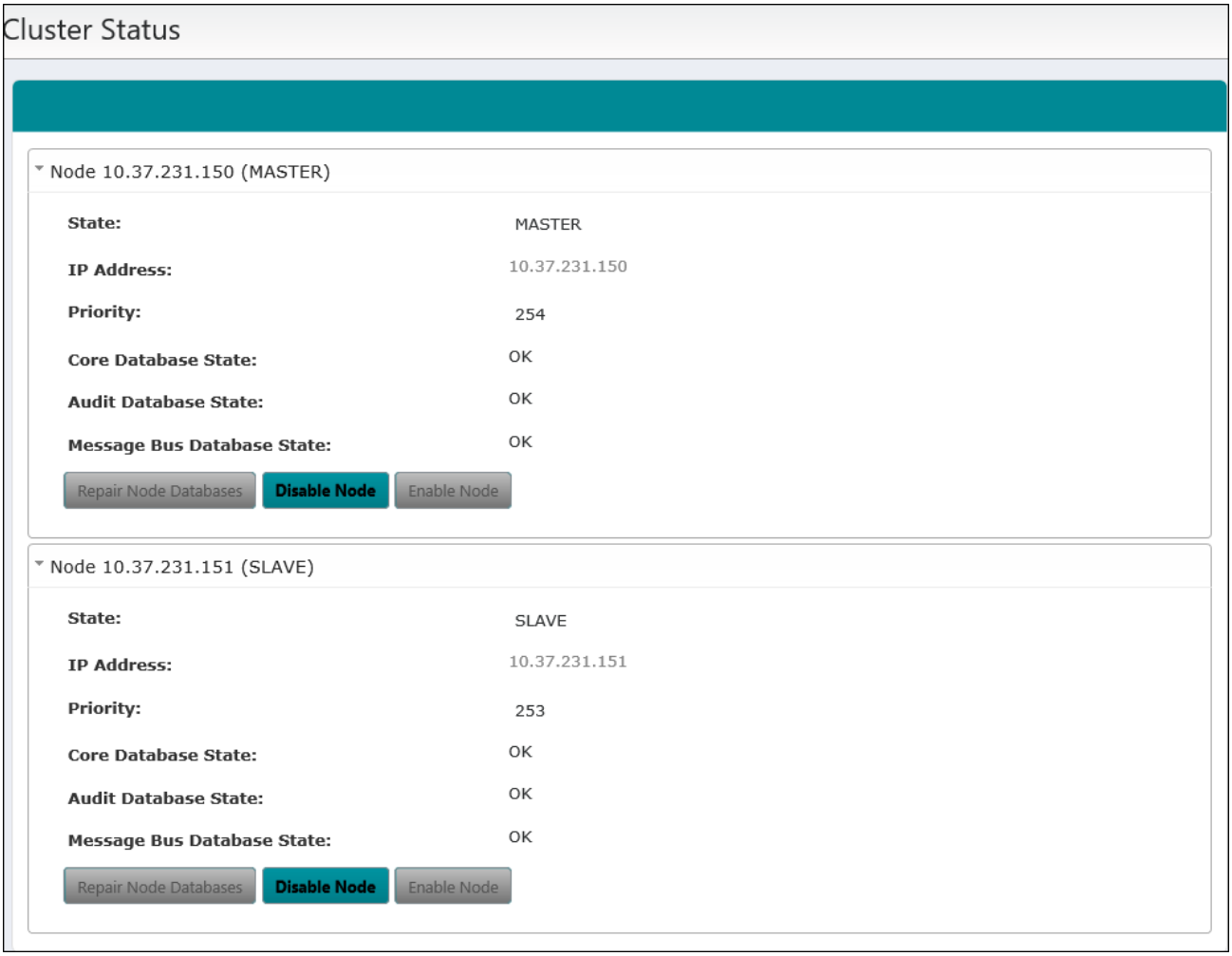
View the state of each node and the status of the core, audit, and message bus databases.

If a database on a node is out of sync, the system displays an option to repair the node's database(s). You can also enable or disable nodes from the **Database Cluster Status** section.

1. Navigate to the **Status** section in the navigation bar and select **Database Cluster Status**.
   The Master and Slave nodes in the database cluster are displayed with their IP addresses.

Note: If your system is set to be in a standalone state, then the database cluster status is not displayed.

2. Click on the Master and Slave node dropdown arrows to view the node status details.
   You can view the current status and priority value for each node, the current network state of each node, and the current state of the Core, Audit, and Message Bus databases on each node.



The following table describes the Database Cluster Status field information:

Field	Description
State	Displays the current state of the node. The State field may display one of the following values: • Start • Master • Slave • Ini_Master • Init_Slave • Disabled • Failed • DB_Repair
IP Address	Displays the IP address of the node.
Priority	The system assigns each node a unique priority value in the cluster within a range of a value between 0 and 255. The value 255 is reserved for the router that owns the IP addresses. When a node is added to the configuration, the highest available priority value is assigned to it. For example, 254, followed by 253, etc.

Field	Description
Core Database State	Displays the current database replication status of the Core database on the node.
Audit Database State	Displays the current database replication status of the Audit database on the node.
Message Bus Database State	Displays the current database replication status of the Message Bus (OpenMQ) database on the node.

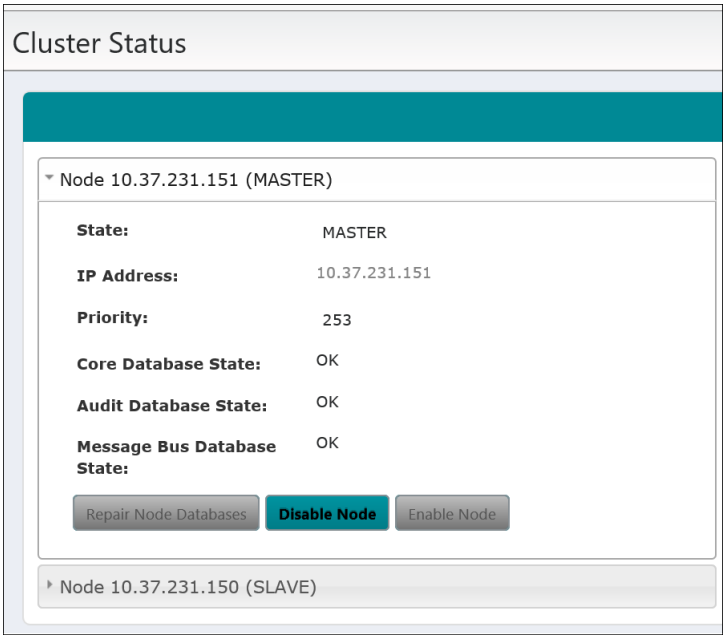
Failing Over and Repairing Database Clusters

Learn how to repair and restart the Database cluster.

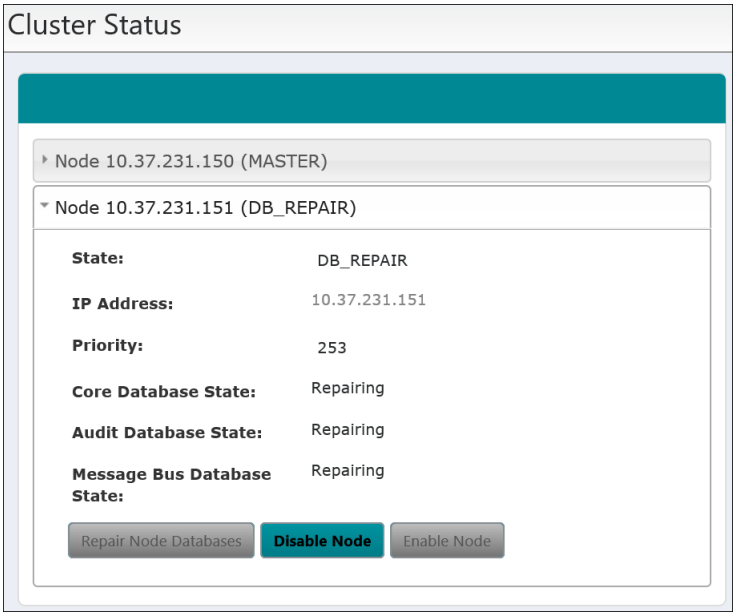
You can use the **Database Cluster** in the **Status** section of the Web Console to failover and repair the current master cluster.

To failover and restart the cluster:

1. Navigate to the **Status** section of the navigation bar and click **Database Cluster** to display the Database Cluster page.
2. Click on the Node (Master) drop down to display the node status.
3. Click **Disable Node** to failover the cluster from the current Master node to the Slave node.
   For example, if the Node (Master) is 10.37.231.151, clicking **Disable Node** will fail over this node to the Node (Slave) 10.37.231.150.



   The system updates dynamically, and the Slave node (10.37.231.150) is displayed as the new Master node. The previous Master node's status changes to **Disabled** state.
4. Click the Node (Slave) drop down to display the node (Slave) status.
5. Click **Repair Node Databases** to bring the node back to an operational state.
   The Node (Slave) or former Node (Master) status changes to **DB_Repair** mode. Status for all three databases (Core, Audit, and Message Bus) also displays the **Repairing** state.



Tip: Wait for the system to finish the database repair process and update the database status.

6. Click the Node (Slave) drop down to view the status of the repaired databases.
   If all three databases display an **OK** status, then the Master and Slave nodes are now fully repaired and operational.

Voice Cluster

The Vocera Voice Service automatically configures the voice clusters behind the scenes when you configure database clustering. The Vocera Platform uses the same IP addresses to designate the active and standby voice clusters.

In voice clustering, a node relies on the discovery mode to determine if an active node is available. Each standby node in a cluster periodically polls the active node to synchronize transactions. If the standby node does not receive a response within 10 seconds, it assumes that the active node has failed and enters the discovery mode to check the status of other nodes in the cluster.

If no cluster member is active and no other server is in discovery mode, the standby server comes online as the active node and takes control of the cluster. When an active node is discovered, it performs a remote restore and then goes into Standby mode.

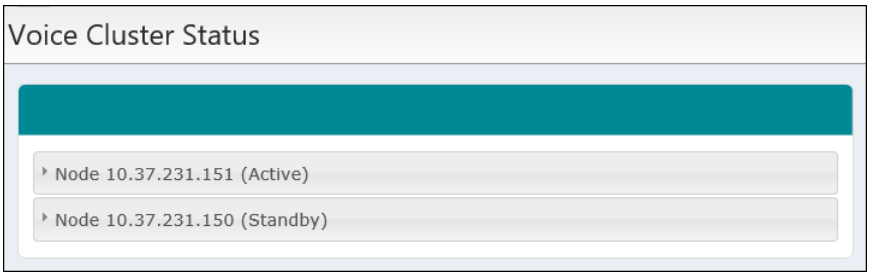
Note: Once the voice clusters are configured, you can use the **Voice Cluster** in Status section of the Vocera Platform Web Console to restart, and monitor the status of the voice clusters.

Viewing Voice Cluster Status

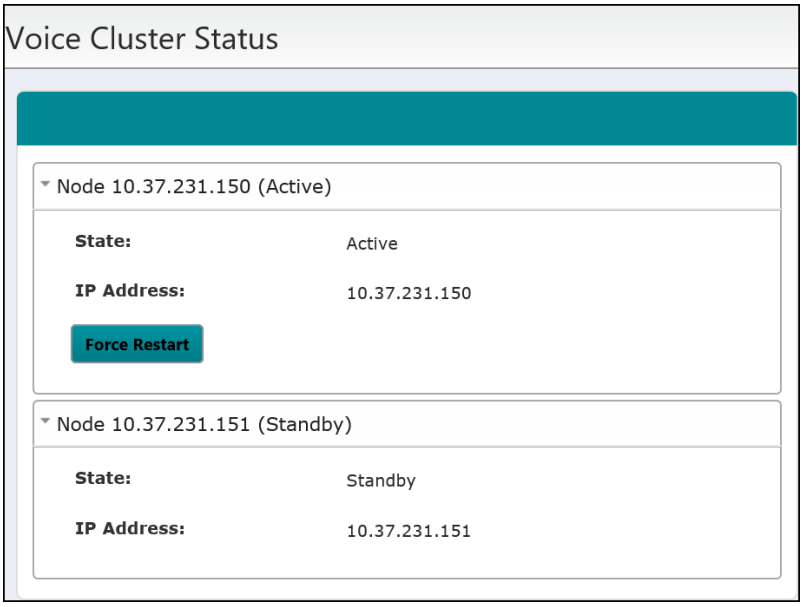
View the state of each node in a voice cluster.

You can navigate to the **Status** page in the Vocera Platform Web Console to view the current information on the state of each node in the cluster.

1. In the **Status** page, navigate to **Voice Cluster**.
   The Active and Standby nodes in the voice cluster are displayed with their IP addresses.



2. Click on the Active and Standby node drop down arrows to view the node status details.
   You can view the current status and IP addresses for each node.



The State field may display one of the following values:

- Active
- Standby
- Failed
- Unknown
- Restoring

Failing Over and Restarting Voice Cluster

Learn how to perform a failover or restart the voice cluster.

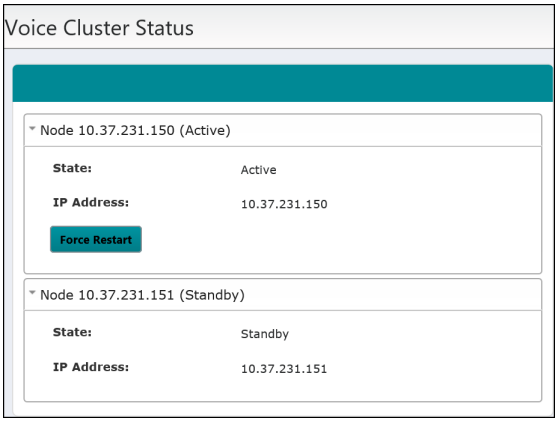
Before you begin the voice cluster management through the Vocera Platform Web Console, you must configure the required network settings as described in the Editing Network Settings on page 325.

You can use **Voice Cluster** in the **Status** section of the Web Console to failover and restart the current master cluster.

To failover and restart the cluster:

1. Navigate to **Status** and click **Voice Cluster** to display the Voice Cluster Status page.
2. Click on the Active node drop down to display the node status screen.
3. Click **Force Restart** to failover the cluster management from the current Active node to the Standby node.

   For example, if the Active node is 10.37.231.150, clicking **Force Restart** will fail over this node to the Standby node 10.37.231.151.



The system updates dynamically and the Standby node (10.37.231.151) is displayed as the new Active node.

Wait a few minutes to allow the system to finish the restore process.

The previous Active node's status changes to **Restoring**, and finally to **Standby** state.

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 performs 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:

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—voice service, 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 voice service on the active node fails, resulting in the following events:
   - The voice service 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 multiple nodes are in discovery mode at the same time, the node at the top of the list 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 voice service node 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 voice service cluster 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.

After badges have received the initial list of cluster members, you can maintain it by updating the `badge.properties` file on the active node.

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:

- 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 — synchronizes 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:

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.
Report 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 voice service 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. **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 voice service during any process. The following table provides details about the unsynchronized files:

Type of Data	Reason not Synchronized
The `properties.txt` file	Each Vocera Platform may require hardware-dependent settings in `properties.txt`. Each Vocera Platform may require different logging parameters in `properties.txt`.
Vocera Platform 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 constantly communicate 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 voice service cluster communication. Files are not relevant from one machine to another.

Network Problems and Clustering

The flexibility of a distributed cluster architecture requires you to have a stable network environment.

Vocera Platform clustering provides a distributed architecture that allows you to locate nodes anywhere on your network, including different subnets and different geographic locations (as described in Geographically Distributed Clusters on page 134). 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:

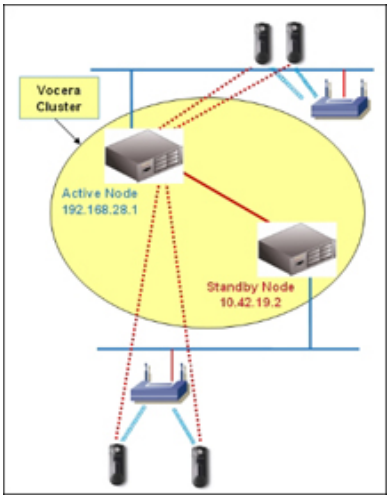


Figure 1: Simple cluster with one active and one standby server

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:

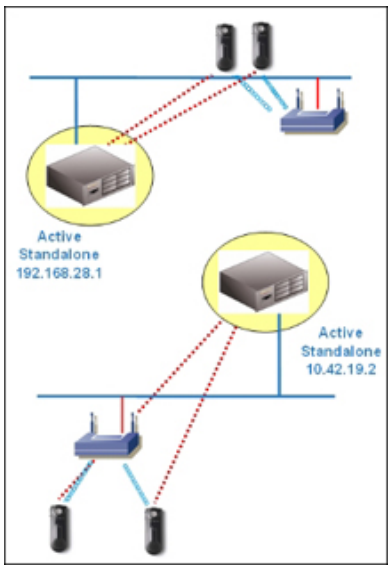


Figure 2: Simple cluster with two active servers (a "split brain" state)

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, voice service 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 134 for a discussion of disaster recovery.

To disable the self-healing mechanism:

1. On each cluster node, 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 voice service.
   a. Stop and start the standby node(s). 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 357 let you know that unknown events are affecting your cluster.

Table 1: 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.
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.

Planned Network Outages

Follow these steps to prevent failovers, a split brain, or an interruption to voice 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 interruption to server, except for badges that cannot find a path to the active node because they were isolated by the outage.

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:

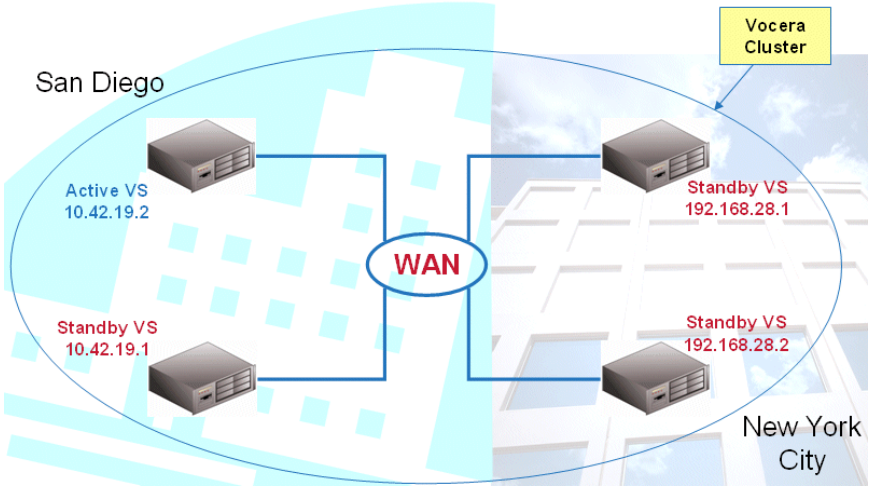


Figure 3: Geographically distributed cluster

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:

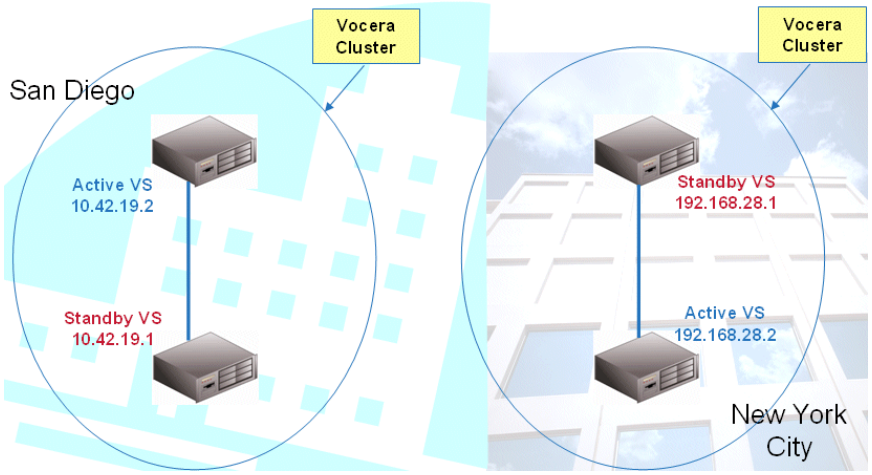


Figure 4: Geographically distributed cluster after a WAN failure

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, voice service 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 2: 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.
Report logs.	No. The voice service logs 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.

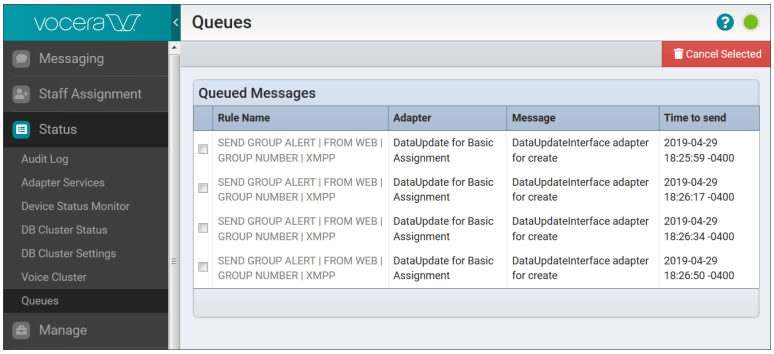
Queues

Access the list of messages that are currently being processed for delivery, or are waiting to be processed, on the Vocera Platform.

Messages that display in Queues have had their delivery deferred; for example, due to a secondary/tertiary escalation path configuration or a fail-over condition.

In Queued Messages, you can view messages that have been sent, but are not yet delivered. On this page, you can identify the rule, adapter, message contents, and time to send values that were configured to send the selected message. The functionality provided in Queues allows users to refresh a selected message, or to cancel message processing if desired.

In the Vocera Platform Web Console, navigate to **Status > Queues** to display the Queued Messages page.



The fields in Queued Messages are described below.

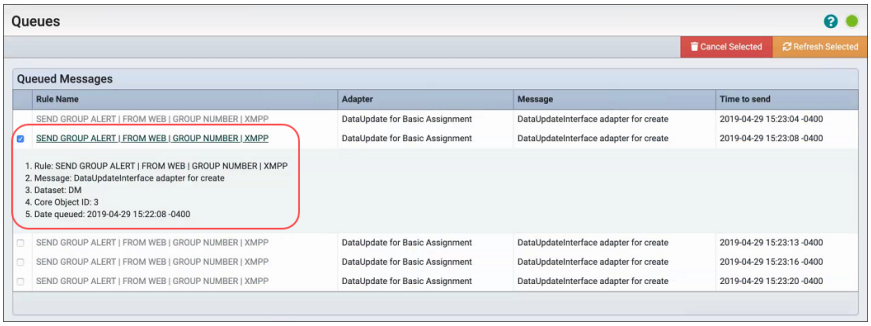
Field	Description
Rule Name	Displays the name of the rule that triggered the message to be sent.
Adapter	Displays the reference name of the adapter on which the rule is based. The adapter is selected in the rule configuration.
Message	Displays the message contents.
Time to send	Displays the Time to send value, which is configured in the rule that triggered the message to be sent.

Viewing Queued Message Detail

In Queues, you can select a message to view its processing details.

In the Vocera Platform Web Console, navigate to **Status > Queues** to display the Queued Messages page.

1. Select a message by checking the box located on the left of the Rule Name field.



The details for the selected message display below the entry in the Queued Messages table.

2. View the details of the queued message fields described in the table below.

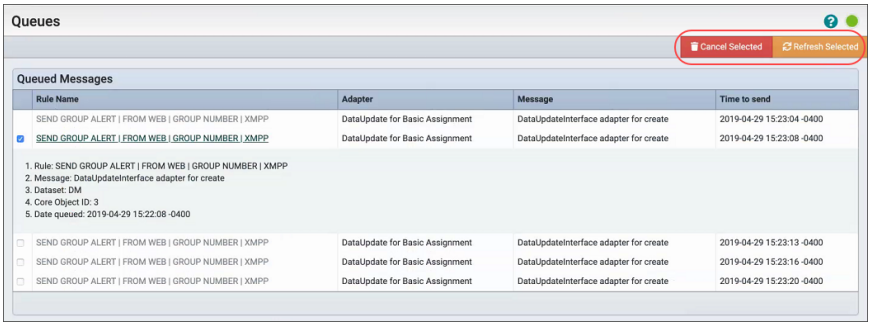
Field	Description
Rule	Displays the name of the rule that triggered the message to be sent.
Message	Displays the message contents.
Dataset	Displays the name of the dataset on which the rule was created.
Core Object ID	Displays the dataset core object ID for the message.
Date queued	Displays the date and time that the message entered the queue. In the example above, the message will be sent in one minute; it entered the queue at 15:22:08, and its configured Time to send value is 15:23:08.

Canceling a Queued Message

In Queues, you can select a queued message and stop its delivery process.

In the Vocera Platform Web Console, navigate to **Status > Queues** to display the Queued Messages page.

1. Select a message by checking the box located on the left of the Rule Name field.
2. Select an action from the menu for the selected message, as needed.



3. Choose an action as described below.
   - Cancel Selected—Cancel delivery of the selected message on the Vocera Platform.
   - Refresh Selected—Update the selected message display to current status.

Manage

The **Manage** section of the **navigation bar** in the Vocera Platform Web Console allows you to perform typical administrative tasks such as managing users, groups, and facilities.

- Users on page 140
- Groups on page 166
- Facilities on page 186
- Contacts on page 222
- Access Point (AP) Locations on page 228
- Device Inventory on page 234
- Templates on page 248
- Bulk Actions on page 254

Users

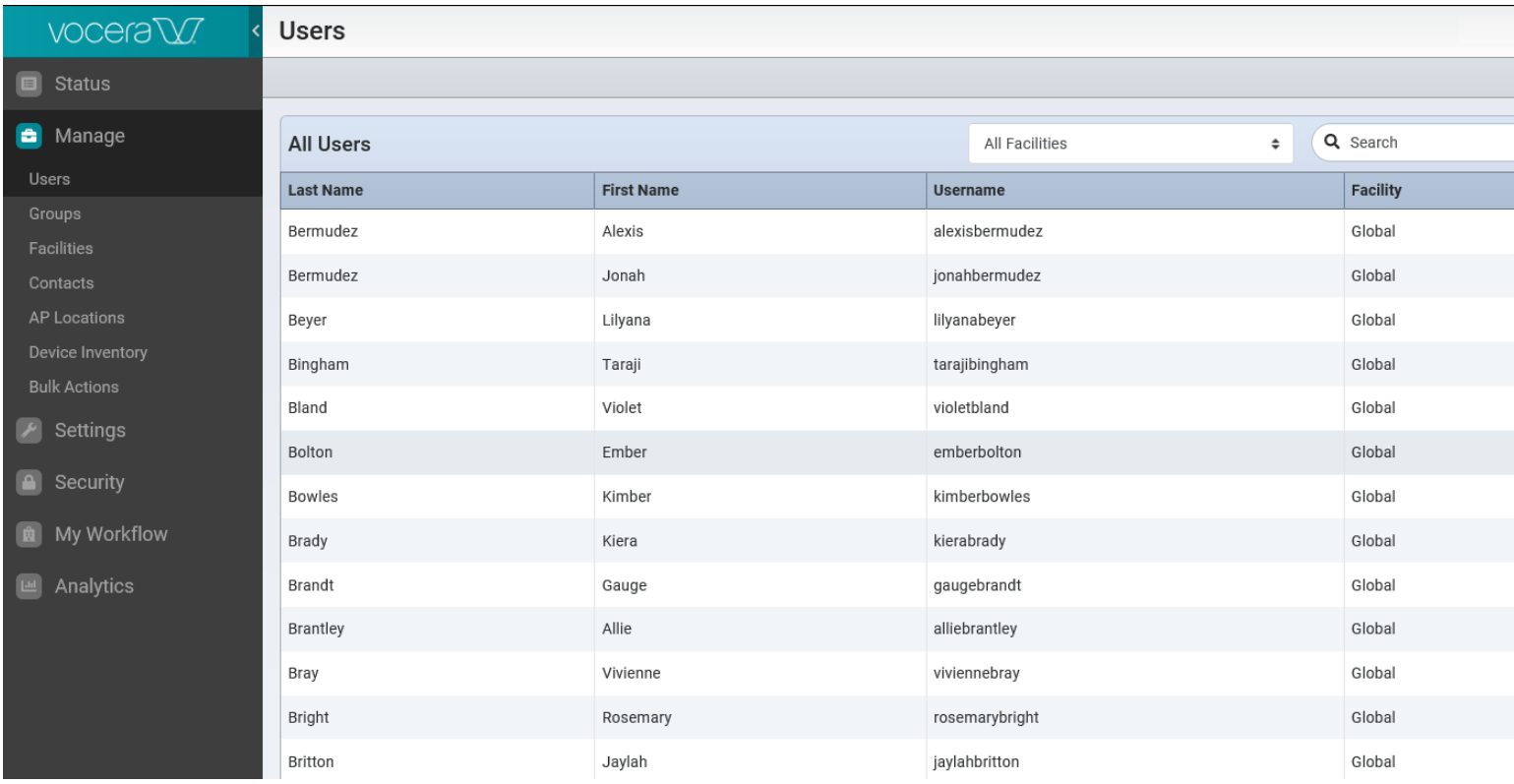
Use the Vocera Platform Web Console to view and manage all users in the system.

A user is an entity that you create in the Web Console to represent a person who uses the Vocera system. All users have a name and log-in credentials.

System administrators can manage users and perform the following tasks:

- Add a single user or multiple users
- Modify user information
- View a user's profile information
- Reset passwords or PIN (if applicable) for selected users
- Search for a user
- Sort users for a selected facility

To view all the user in your system, select **Users** in **Manage** section of the navigation bar. The All Users page displays with a list of users in alphabetical order with their last name, first name, username, and facility information.



As a system administrator, you can also access the user profile details. You can search for a user using the Search bar. See Searching for Users for additional information on the Web Console search capabilities.

Accessing User Profiles

When you add a user, the Vocera system creates a profile for that user.

You may need to edit the user's profile to add features that may be useful or remove features that a user doesn't require. In addition to a user's name and contact information, the user preferences such as preferred Genie persona, speech recognition, and memberships are stored in the profile information.

You can use any of the following methods in the Web Console to add user profiles:

- Add one user profile at a time, see Adding a User for additional information.
- Add a large number of users, import them directly using a CSV (comma separated value) file. See Importing Data to the System for additional information.

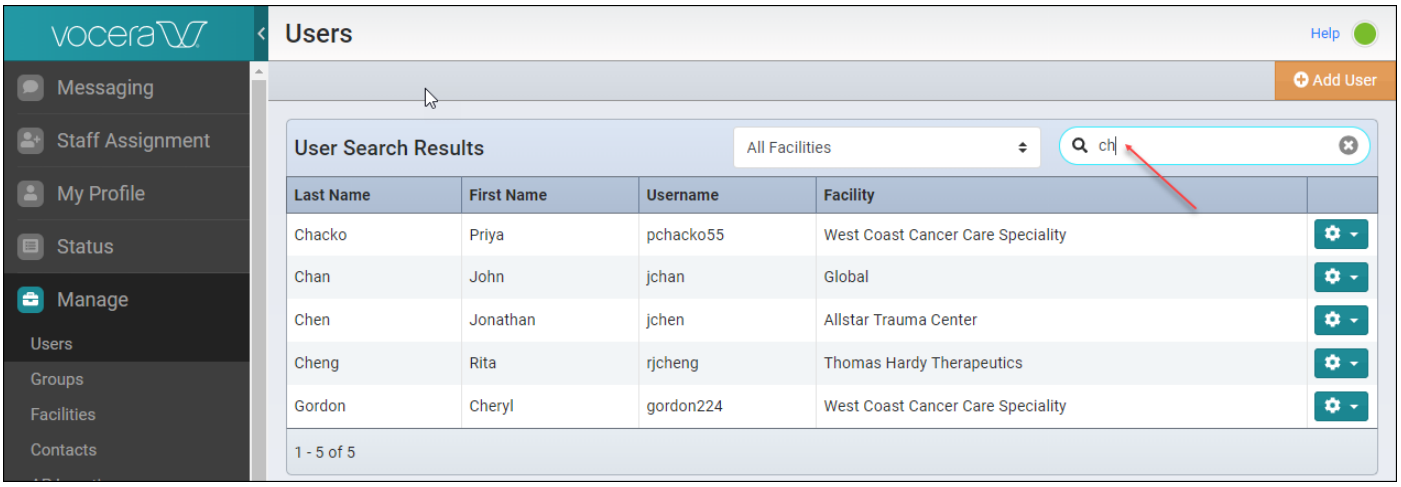
Searching for Users

You can use the Web Console Search bar to locate users in a specific facility or across all facilities in the system.

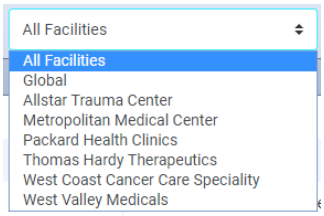
System administrators may need to locate users across facilities to add, remove, or configure settings for users.

1. Click **Users** in the **Manage** section.
   All users in the default All Facilities are displayed.
2. Enter one of the following in the Search bar:
   - Username
   - First Name
   - Last Name

   As you start entering the Username, First Name, or Last Name, the search immediately pulls any records for these fields and displays the information.
   For example, if you entered two letters, “ch” in the Search bar, the Web Console Search feature quickly searches for all users with the letters “ch” in their first name, last name, or username and displays all matching records in the User Search Results.



3. Toggle the Facility selector and select the facility in which you want to locate a user



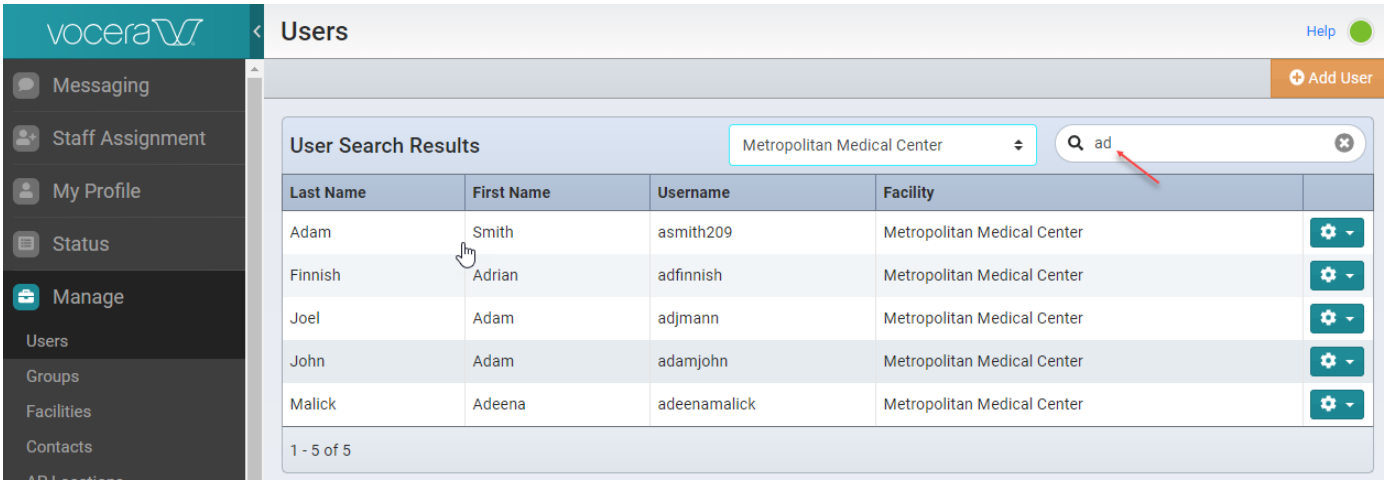
Searching for Users in a Specific Facility

You can filter search results on the username entries by entering a minimum of two letters in the search field.

1. Toggle the Facility selector in the Action bar to sort and display a list of users associated with a specific facility.
2. Enter the first two letters or the complete First Name, Last Name, or Username in the Search bar. If your system is integrated with an existing lightweight directory access protocol (LDAP) directory, you can even use the user's nickname in the Search bar.

   The search immediately pulls any records matching this information and displays all users in the User Search Results.

   For example, if you selected a facility named, “Metropolitan Medical Center”, and start typing the letters, “ad” in the Search bar. The User Search Results will display all user records matching this information as shown in the following screenshot.



Recommended Best Practices for Adding Users

Learn the considerations and necessary tasks to perform before you create users in your environment.

Review and complete the following tasks before you add users to the system:

1. Create individual facilities before creating users so that you can select facilities when you start adding new users. Create individual facilities only if your Vocera system supports users at multiple physical locations. Otherwise assign the user to the Global facility.
2. Create groups and departments ahead of time so that you can select them when you add a new user.
3. Develop a systematic method for assigning a unique user ID to each user. Users enter their user IDs to access My Profile, and they may enter the user IDs of other users to send an email message from a mail client to a device. Here are some possible methods for assigning user IDs:
   - Utilize existing employee ID numbers for creating user IDs.
   - Use existing email addresses, but without the domain reference. For example, if a user's email address isjsmith@yourcompany.com, the user ID could be jsmith.
   - 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 Josh Smith, the user ID could be jsmith.
   - 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.
   - Use the character set of matching the locale when you enter names into the system. For example, Celine may not be pronounced the same way in French locale as Céline. It may, therefore, be necessary to add alternate spoken names (for example",Sailine") or new dictionary entries.
4. Avoid using generic user profiles for Username. 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 voice commands

     Individual users can train the Genie to recognize the way they say names and voice 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 device 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 device.
   - Call by name

     You cannot call a person with a generic profile user name when using the Call by name, locate that person, or even find out if he or she at the Facility.

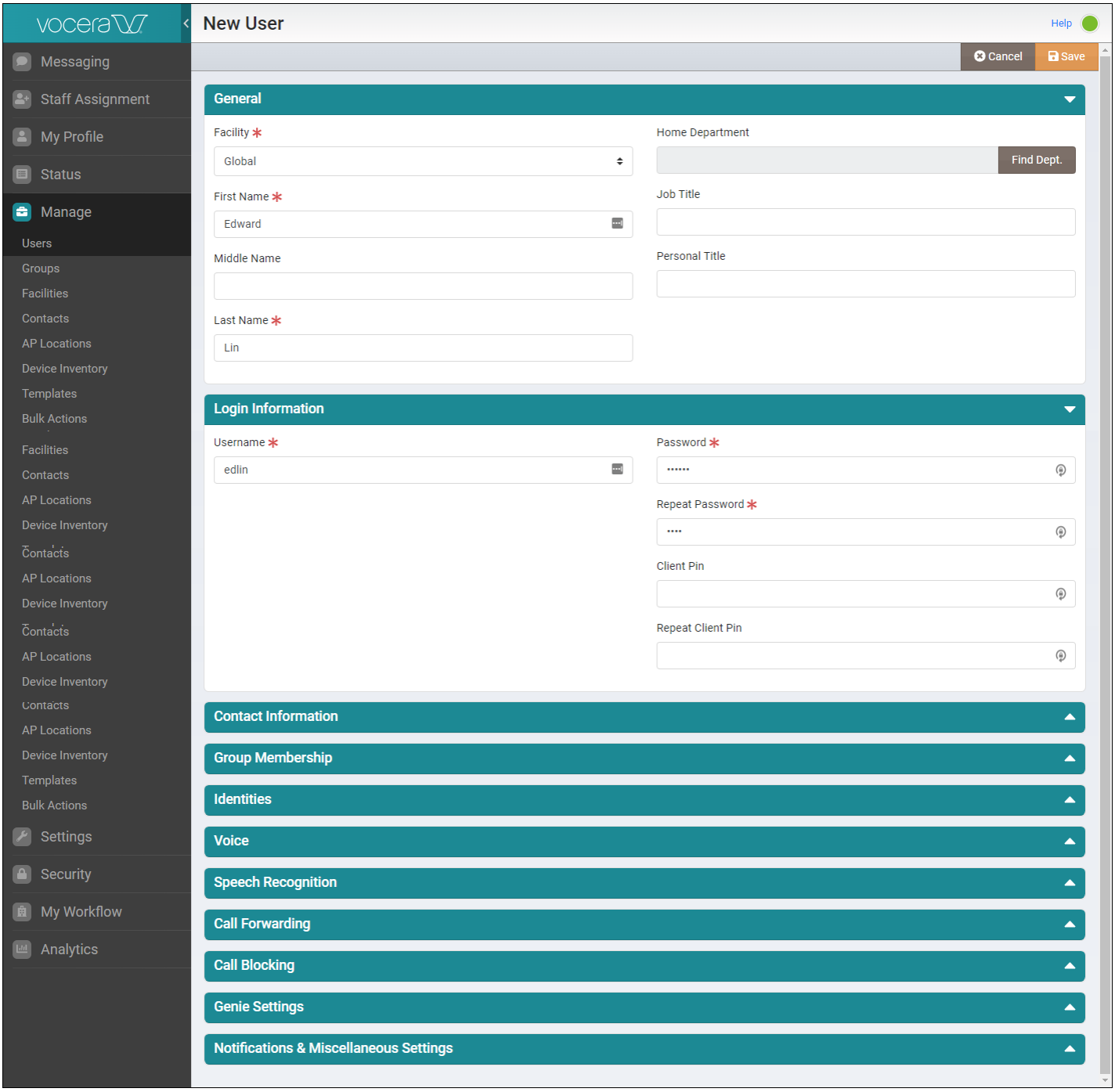
Adding a User

You can add a user to the list of Vocera Platform Web Console users.

Before you begin, review the recommended best practices.

1. Navigate to **Users** in the **Manage** section, and click **Add New**.

   The New User page displays.



The New User page includes the following sections:

- General
- Login Information
- Contact Information
- Group Membership
- Identities
- Voice
- Speech Recognition
- Call Forwarding
- Call Blocking

- Genie Settings
- Notifications & Miscellaneous Settings

Tip: You can click the drop down arrow at the right hand side of each section to expand or collapse these sections.

2. In the General section, complete the fields listed in the table below. An asterisk * indicates that a value must be entered for this field.

   Attention: Vocera recommends that you avoid creating generic user profiles such as," Charge Nurse", "Manager on Call", or "Temp Nurse One" etc. The generic user profiles interfere with basic device 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 device users then have access to all Vocera features, and callers can find them by using either their names or roles.

Field	Maximum Length	Description
Facility *	50	Select the facility associated with your user from the drop down list. If you have not defined a facility, or if you do not want to specify a facility for the new user, select the default **Global** value If your organization has multiple facilities connected to the same Voice Service, choose the facility that represents the user's physical location.
First Name *	50	Enter the user's First 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 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 section.
Middle Name	50	(Optional) Enter the user's middle name. The middle name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed.
Last Name *	50	Enter the user's last name. The last name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed.
Home Department	50	Click **Find Dept.** to display the Find a Department dialog box and select a home department for this user. If your organization has multiple facilities connected to the same Voice Service, choose the facility that represents the user's physical location.
Job Title	100	(Optional) Enter a job title for the new user. Provide the full spelling of the title rather than an abbreviation. For example, enter Professor instead of Prof.
Personal Title	100	(Optional) Enter a personal title for the new user. For example, Mr., Ms., Mrs.

3. In the Login Information section, complete the fields listed in the table below. All fields must be provided.

Field	Maximum Length	Description
Account Enabled *	N/A	This field is visible only when editing a user; when you initially create a user, the field does not appear and the account is enabled by default. Disabling an account is useful in situations where a user is temporarily not available. When the account is disabled, the user's name and alternate spoken names are removed from the system grammar, improving speech recognition; in addition, disabled users do not decrement your overall user count for licensing purposes.
Username *	50	Enter the username that the new user will use to log in to **My Profile**. Minimum length for username is 4 characters and maximum is 50 characters. You can only use letters, digits, underscores (_), or dashes (-) in your username. No other characters are allowed.
Password *	64	Specify a password for the user's **My Profile** login credentials. Minimum length for password is 4 characters and maximum is 64 characters. You can only use letters, digits, common punctuations, and symbols in your password. No other characters are allowed.
Repeat Password *	64	Re-enter the password. Must be identical to the value entered in the **Password** field.
Client Pin	Varies per PIN policy	Enter a numeric value for Client PIN. See Understanding the PIN Authentication Security Items for more information on PIN policy.
Repeat Client Pin	Varies per PIN policy	Re-enter the Client PIN number.
Reset Client Pin	Varies per PIN policy	Allows to reset an existing Client Pin and add a new Client Pin Click Reset Client Pin link to display the Reset Client Pin dialog box. 1. Specify a client pin in the **New Client Pin** field. 2. Re-enter this pin value in the **Repeat Client Pin** field. 3. Select **Reset** to proceed with the client pin reset action.

4. In the Contact Information section, optionally complete the fields listed below.

Field	Maximum Length	Description
Email Address	60	Enter the user's email address to facilitate the following: Other users can send voice messages from their devices 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. .
Cell Phone	50	Allows users to forward calls from a device 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 devices to their home phones. It also allows users to take advantage of the “Call My House” Contacts entry.
Employee ID	50	Specify an employee ID (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
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, outside callers can 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 devices. • 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.
Pager	50	Allows users with the proper permissions to receive numeric pages on their pagers from other device users who issue the "Page" voice command.
Cost Center	100	Specify a cost center to which the new user is assigned. A cost center ID lets Vocera track system usage by users and potentially allows an organization to charge for relative usage.

5. In the Group Membership section, add the user's group membership information.
   a. Click **Add Group** to display the Select Group dialog box.
   b. Select a group name from the list of groups available in the system.
   c. Click **Select Groups** or **Cancel** to close the dialog. .
      You can add multiple groups to this user's profile
   d. Click **Find Group** to add groups for **Conference Group this user is a member of** field.
      The **Conference Group this user is a member of** field allows you to add members of a group or groups who's devices are activated when you perform the push and hold function on the device. This feature is useful in situations where you need an immediate communication and voice recognition (Genie) is not involved.
      A user can only belong to one conference at a time even if the user is a member of multiple groups.
6. In the Identities section, click **Add Identity** to associate a unique alternate identity for a user.
   Alternate user identities are system generated and connected to an adapter or a service. Occasionally, system administrators may need to delete or update this field for a user.
   When you click the **Add Identity** button, the Add Identity dialog box appears. In the Add Identity dialog box:
   1. Enter a name in the **Name*** field.
   2. Select an Adapter from the **Adapter** drop down list and click **Done**.
   3. Repeat this step to add additional identities for this user.
7. In the Voice section, complete the fields listed below:

Field	Maximum Length	Description
Vocera Phone	50	Allow users to forward calls from their Vocera devices to the specified phone number. 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.
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 facilities. A PIN template can include digits, special characters, and PIN macros.
Device ID	12	Enter the MAC address of the device. This is available on the device's **Info** menu. The MAC address of a device is also printed near the bottom of the white label under the battery.For Vocera devices, 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.
Enable Access Anywhere	n/a	**Important:** Unless you have enough Vocera Access Anywhere licenses for all of your users, Vocera recommends that you leave this default setting cleared. When selected, the **Enable Access Anywhere** option enables the 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. If you check this box, make sure you enter a password in the **Phone Password** field for all users that are not authenticated by Caller ID when they access the Genie from a phone. Also, re-enter the password in the Repeat Phone **Password** field. 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 explicitly been enabled to use the Vocera Access Anywhere feature can take advantage of it.
Phone Password	25	Password used to authenticate the user when accessing the Vocera Genie from a phone. The Phone Password must be five to 25 characters consisting of letters or numbers. Special characters are not allowed.
Repeat Phone Password	25	Re-enter the password that you entered in the **Phone Password** field.

8. In the Speech Recognition section, optionally enter the following fields.

   By default, it is assumed that users will be called by their first and last names. Enter Alternate Spoken Names only if:

- People call the user by different names (such as “Bill Smith” in addition to “William Smith”)
- The user's name is pronounced differently from the way that it is spelled. In this case, add one or more phonetic spellings.

Field	Maximum Length	Description
Doctor Prefix	n/a	Select the Doctor Prefix check box to indicate the user is a Doctor. If you are using this option, you do not need to enter Doctor prefix as a value for one of the **Alternate Spoken Name** (ASN) fields. For example, if you selected **Doctor Prefix** field for a user named, “John Smith,” you can use a voice command, “Call Dr Smith” on your device. Vocera speech recognition will quickly recognize this voice command and call the user named John Smith.
Enable Frequently Called User	n/a	Enables or disables this user to be included in the weighting for improving speech recognition for frequently called users and departments. **Attention:** This option is used in conjunction with the system-level configuration for frequently called users. You can select this option only when you have selected the **Preferences > Favor Frequently Called > Users** field in the **System Configuration** section.

Field	Maximum Length	Description
Alternate Spoken Name #1	50	Enter an alternate spoken name. Use these guidelines to ensure the best result when you are defining alternate names for users: • **Person, Group, and Location Names** — If users refer to a person, group, or location 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. • **Digits in Name Fields**— 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 these special characters are allowed, it is unlikely that an alternate spoken name would need underscores (_), or dashes (-). • **Staff IDs** — It is recommended that you do not create an alternate spoken name that contains numeric digits only. For example, a staff ID with numbers and no letters. `567748` Entering numeric staff IDs are permitted. However, using numeric values only might result in • Slower Genie response times • Problems with phone number recognition • **Acronyms and Initials in Alternate Spoken Names**— If people use an acronym or initials to refer to a contacts 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. For Jasdeep Narindar Singh, also enter J N Singh rather than J.N. Singh. • **Unusual Pronunciation**— If a name has an unusual or confusing pronunciation or silent letters, 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. • **Professional Titles in Alternate Spoken Names**— If users refer to a person by his or her title, provide the full spelling of the title rather than an abbreviation. For example, enter Father Brown instead of Fr. Brown, or Professor Lindsay instead of Prof. Lindsay. • **Doctor Title in Alternate Spoken Names**— When adding or editing user profiles, you do not need to include the Doctor title as part of the user's name in the Alternate Spoken Names (ASN) field on the Speech Recognition tab. Instead, check the Doctor Prefix check box. When you speak a command using one of the ASN variations, Vocera understands the user to whom you are referring. For example, when you speak, Call Doctor Michael Smith, the Vocera Genie knows that you are referring to Doctor Michael Smith. You could also speak, Call Doctor Smith or Call Doctor Michael and the Genie will find the user because the Doctor Prefix option is checked.

Field	Maximum Length	Description
Alternate Spoken Name #2		The second alternate spoken name, if needed.
Alternate Spoken Name #3		The third alternate spoken name, if needed.
Identifying Phrase		Optionally, specify a phrase that distinguishes this user from others with the same first and last names. For example, "Bill Smith in Marketing." and "Bill Smith in Finance"

9. In the Call Forwarding section, select the **Enable Forwarding** checkbox to see the forwarding related fields. Optionally, specify where incoming calls are to be forwarded.

   Choose one of the following to specify where incoming calls are forwarded:

   - Forward to Company Voice Mail (default)
   - Forward to Another User, Group, or Contact
   - Forward to Desk Phone
   - Forward to Cell Phone
   - Forward to Home Phone
   - Forward to Another Number

   See Forwarding Calls for more information on configuring forwarding options.

   Choose a condition to specify when to Forward the calls:

   - **All** — When selected, all calls are forwarded without an alert tone or ring on your device.
   - **Unanswered** — When selected, all unanswered calls are forwarded. This is also the system default.
   - **Offline** — When selected, forwarding occurs only when you are not logged in, or are off the network.

10. In the Call Blocking section, specify whether to **Allow all calls by default** or **Block all calls by default**.

    You can also add call exceptions to the user's settings. See Adding Call Blocking Exceptions for more information.

11. In the Genie Settings section, configure the Vocera Genie, which is the voice interface between the user and the Vocera Platform. 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.

    Optionally enter the following settings:

Field	Description
Genie Voice	Click a radio button to choose a persona for Genie voice. You can click the preview icon by a persona name to play a sample. A Genie voice is a set of voice prompts and tones that give the voice interface a distinctive identity. The default **Genie Persona** varies per locale, and **Override User Settings** is set to **No**
Genie Greeting	A device 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** • **Tone and Speech** Click the icon next to the choice to play a sample greeting. By default the **Speech only** option is selected, and **Override User Settings** is set to **No**
Call Announcement	In the **Call Announcement** section, choose a **Ring Tone** from the list. Click the icon next to the Ring Tone selector to play a sample. By default, the selected ring tone is Ring-Tone-01, and **Override User Settings** is set to **No**.

Field	Description
Announce caller's name after tone	Select this checkbox if you want the user to hear who is calling. This announcement adds to the time required to connect each call. By default, the **Announce Name of Called Group** 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 facility to which this group belongs (if it is different from the caller's facility) 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 facilities, the Genie says, "Call to [GroupName] at [FacilityName] from [CallerName]. Accept?" By default, the **Announce Name of Called Group** box is selected, and **Override User Settings** is set to **No**.

12. In the Notifications & Miscellaneous Settings section, specify the notifications and settings not covered in the other sections.
    a. Specify alert tone settings in the **Alert Tones** section:

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 Alerts in DND Mode	**Disable Alerts 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 not selected, and **Override User Settings** is set to **No**.

    b. Choose any reminders you want to enable in the **Reminders** section:

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 not selected, 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**.

    c. Choose any notifications you want to enable in the **Automatic Notifications** section. Automatic notifications allow users to bypass certain operations without confirming them.

Setting	Description
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. Users may prefer to use the "Who called?" command when they are in a quiet area to learn who called. If users are trained to do that, you can clear the **Missed Call Notification** setting. 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 not selected, and **Override User Settings** is set to **No**.

d. In the **Message Play Settings** section, specify the behavior of the "Play Messages" commands.

Setting	Description
Play Older Messages First	**Play Older Messages 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 not selected, 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 not selected, and **Override User Settings** is set to **No**.

e. In the **Call Setup** section, specify the behavior of the call setup.

Setting	Description
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, "Can you talk to [*CallerName*]?" 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**.

Setting	Description
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**.
Press Button to Accept Call	Use the **Press Button to Accept Call** setting to require 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 accept or reject calls without user input prematurely. To avoid these problems, select this box to require users to answer calls using buttons only. By default, the **Press Button to Accept Only** box is not selected, and **Override User Settings** is set to **No**. Enabling this feature establishes a new system-wide default and may require re-training.
Enable Paging	Enable the Vocera Access Anywhere paging capability. By default, the Enable Paging box is selected, and Override User Settings is set to **No**.

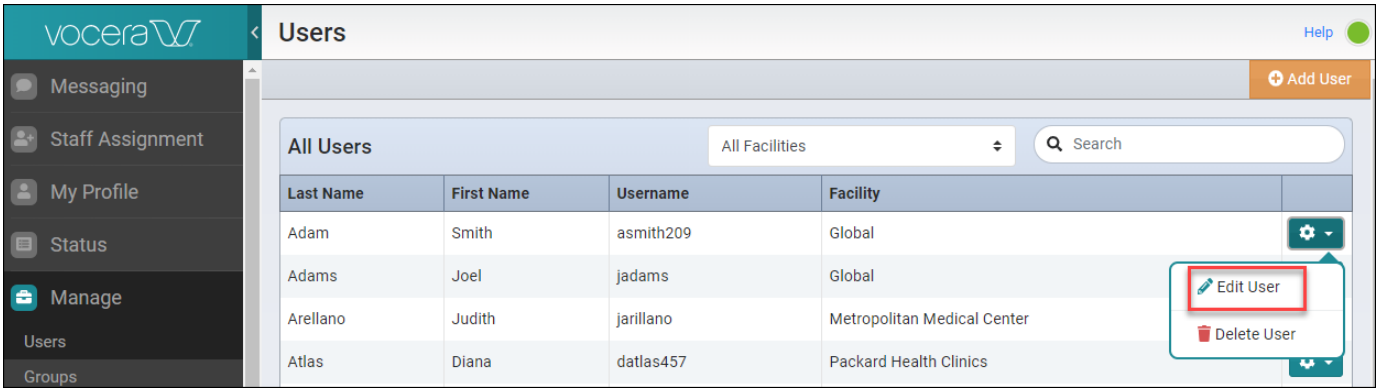
13. Select one of the following to close the dialog:
    - **Save** — to add the new user to the system.
    - **Cancel** — to return to the All Users page.

Editing a User

You can edit the information for any existing user in the system.

1. Click **Users** in the **Manage** section.
   All users for the selected Facility are displayed.
2. Locate the user that you want to edit.
3. Click the **Options** button in the far right of the user that you want to edit.

4. Select **Edit User** from the dropdown menu.



The Edit User page displays with information for this user.

5. Edit the user information as necessary. See Adding a User on page 143 for a list of the user fields.
6. Select one of the following to close the dialog:
   - **Save** — to update the user information in the system.
   - **Cancel** — to return to the All Users page.
   - **Delete User** — to remove this user from the system permanently.

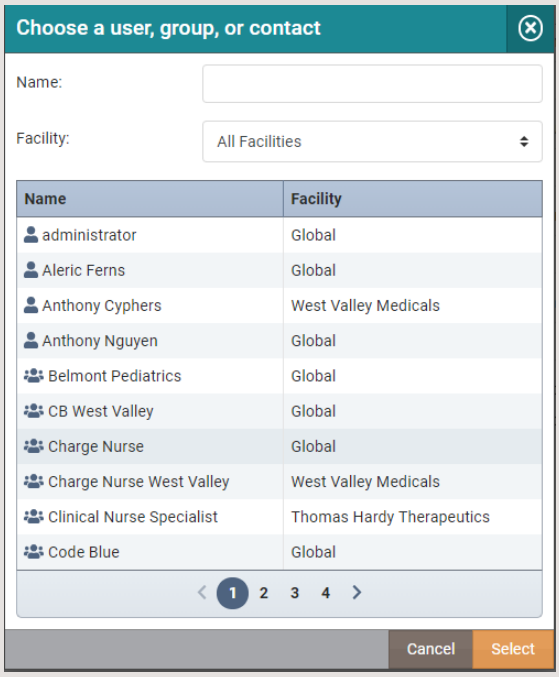
Forwarding Calls

Modify user settings to enable call forwarding features for a specific user.

Forwarding calls is helpful when you cannot answer a call for any reason, or when you block all calls or put your device in Do Not Disturb mode; your caller is usually prompted to leave a message.

1. Click **Users** in the **Manage** section to display All Users page.
2. Click on the User that you want to edit for the forwarding settings.
   The Edit User page displays
3. Scroll down to the **Call Forwarding** section in the Edit User page.
4. Select **Enable Forwarding** to display call forwarding fields.
5. Choose one of the following to specify where incoming calls are forwarded:

Forwarding Options	Descriptions
Forward to Company Voice Mail (default)	Select to forward the unanswered call to your company voice mail.

Forwarding Options	Descriptions
Forward to Another User, Group, or Contact	Select to forward the unanswered call to another user, group, or contact. If you selected **Forward to Another User, Group, or Contact**, Click the **Choose** button to display the Choose a user, group, or contact dialog box with a list of all the choices available in the system.  You can enter the name in the **Name** field to search for a user, group, or contact that you want search in the system. You can also use the **Facility** field to toggle between multiple facilities available in your system and refine your search. Click **Select** or Cancel to close the dialog box.
Forward to Desk Phone	Select to transfer the unanswered call to the desk phone number saved in the Contacts settings of the user's profile.
Forward to Cell Phone	Select to transfer the unanswered call to the cell phone number saved in the Contacts settings of the user's profile.
Forward to Home Phone	Select to transfer the unanswered call to the home phone number saved in the Contact's setting of the user's profile.
Forward to Another Number	Select to enter another number in the **Forward to Another Number** field.

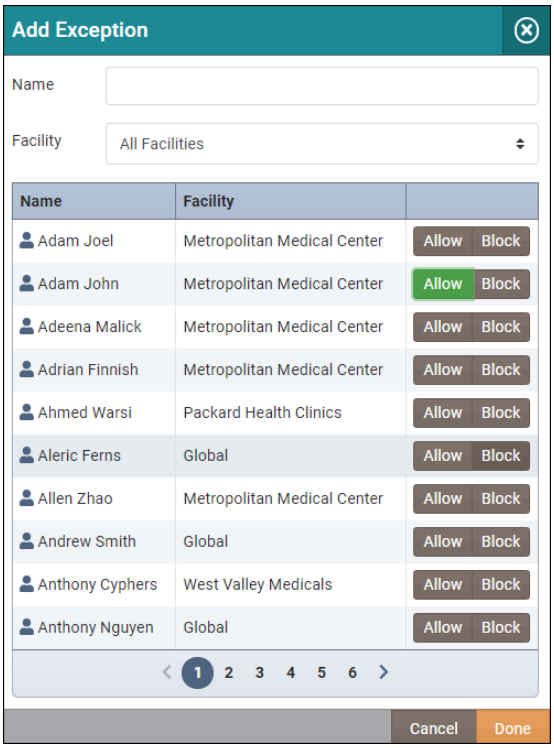
6. Choose a condition to specify when to Forward the calls:
   - **All** — to forward all calls without ringing an alert tone on your device.
   - **Unanswered** — to forward all unanswered calls. This is also the system default.
   - **Offline** — to forward calls only when the user is logged out or off the network.
7. Select one of the following to close the dialog:
   - **Select** — to save the call forwarding configuration.
   - **Cancel** — to return to the All Users page.

Adding Call Blocking Exceptions

Set call blocking exception for selective call screening.

You set the call blocking exceptions for users to allow them to selectively screen callers from whom they want to receive calls or block certain callers.

1. Navigate to **Users** in the **Manage** section, and click **Add New**.
   The New User page displays.
2. Select the user for whom you want to add the call blocking exception.
   Edit User page displays with fields to edit the user's settings.
3. Scroll down to Call Blocking section and select **Block all calls by default**.
   The **Allow all calls by default** is the default settings.
4. Click **Add Exceptions** to display the Add Exception dialog box.

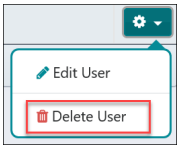


5. Select the **Allow** or **Block** buttons next to caller names that you want to allow or block.
6. Choose one of the following to close the Add Exception dialog:
   - **Done** — to save the selections.
   - **Cancel** — to cancel the selections.
7. Select one of the following to close the Edit User page:
   - **Save** — to update the user information in the system.
   - **Cancel** — to return to the All Users page.

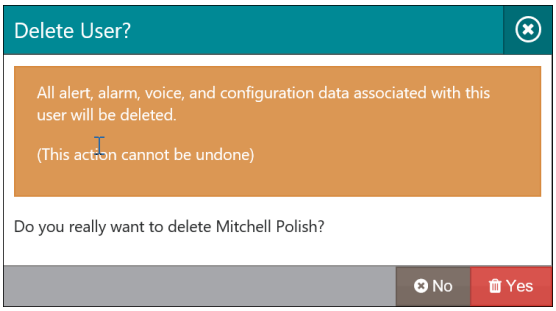
Deleting a User

You can delete an existing user from the Web Console.

1. Navigate to **Users** from the **Manage** section to locate the user that you want to delete.
   The All Users page displays.
2. Locate the user that you want to delete.
   (Optional) You can also use the search bar to locate the user that you want to delete.
3. Click the **Options** button (gear icon) in the far right of this user's row.



4. Select **Delete User** from the dropdown menu.
   The Delete User confirmation dialog displays with the name of the user that you want to delete. For example, the following screen shot displays a Delete User confirmation dialog box for a user named, "Mitchell Polish."



5. Choose one of the following to close the dialog:
   - **Yes** — to confirm the delete action.
   - **No** — to cancel the delete action and return to the All Users page.

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, facilities, locations, contacts entries, and all their possible alternates, such as spellings of user names and the singular and plural names of groups.
  Each facility 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 facility the user is calling. That is, because each facility 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, facilities, AP locations, and contacts, 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, facilities, AP locations, contacts entries can all potentially have alternate names. The following table summarizes the impact of each database entry on the recognition space:

Database Entry	Minimum Spoken Names	Maximum Spoken Names
Empty System	12	N/A
User	4	13
Group	3	6
Facility	8	9
AP Location	2	4
Contacts (Person)	4	11
Contacts (Place)	2	9

Grammars for Facilities

Partitioning a deployment into facilities improves speech recognition, because each facility has its own dynamic grammar, which is the largest component of the recognition space.

When a device user speaks a command, Vocera attempts to process it by combining the dynamic grammar of a single facility with several smaller grammars. Specifically, Vocera searches the following grammars while processing a device user utterance:

- Either of the following dynamic grammars:
  - The dynamic grammar of the caller's current facility
  - The dynamic grammar of the facility to which the caller explicitly connects to
- The Global facility grammar
- The static grammar
- The device user's personal grammar

Vocera always includes the static grammar, the grammar of the Global facility, and the device user's personal grammar while processing the voice commands. However, Vocera includes the dynamic grammar of only a single facility, not the grammars of each facility, while processing the command.

For example, suppose the Central Pacific Resort deployment has two facilities—Carmel and Monterey—in addition to the Global facility. If a device user in Carmel issues the command, “Call Adda Turner”, Vocera uses the following grammars to process it:

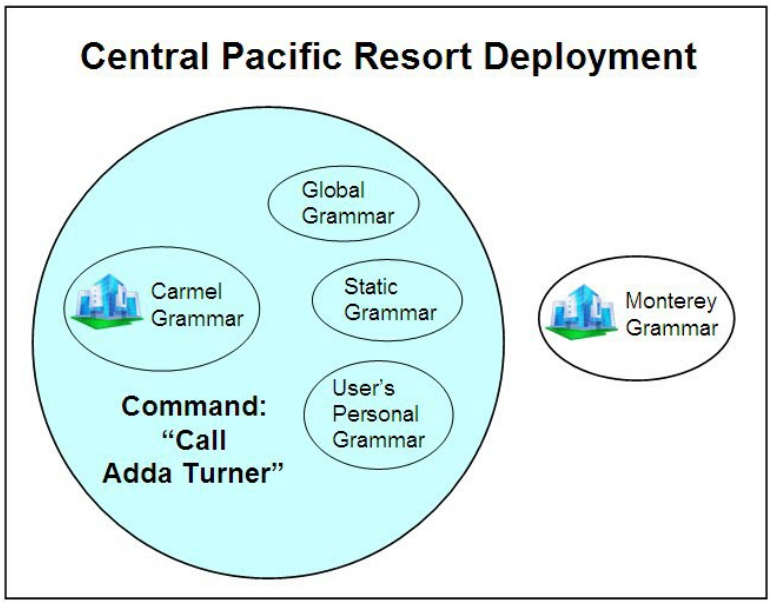


Figure 5: Grammars used at the Carmel facility

Contacting a device user at a remote facility is a two-step process. For example, suppose the Carmel user in the previous example wants to call Adda Turner, but Adda's home facility 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 facility—the current facility 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 facility, as shown in the following illustration:

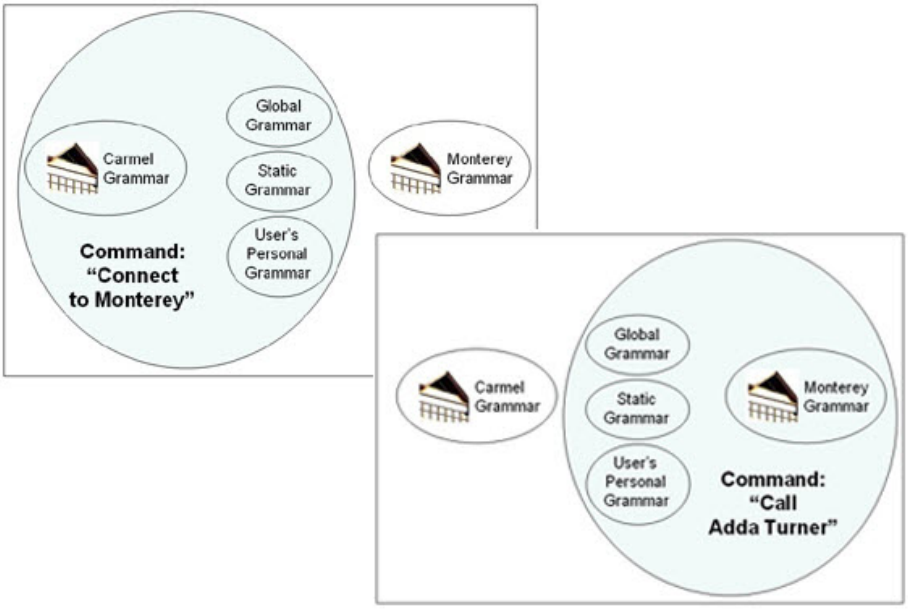


Figure 6: Grammars used after connecting to the Monterey facility

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 facility is not sharing a telephony server, Vocera searches the Global facility grammar and the grammar of the telephony server's facility.
- If the facility is sharing a telephony server and the caller spoke a response, Vocera searches the combined grammars of the Global facility and any facilities associated with the line that the call arrived on.
- If the facility is sharing a telephony server and the caller entered a touch-tone response, Vocera searches the combined databases of the Global facility and each facility that shares the telephony server.

See the Working with Multiple Facilities (in Telephony guide) for more information

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.

Grammars for Facilities

Partitioning a deployment into facilities improves speech recognition, because each facility has its own dynamic grammar, which is the largest component of the recognition space.

When a device user speaks a command, Vocera attempts to process it by combining the dynamic grammar of a single facility with several smaller grammars. Specifically, Vocera searches the following grammars while processing a device user utterance:

- Either of the following dynamic grammars:
  - The dynamic grammar of the caller's current facility
  - The dynamic grammar of the facility to which the caller explicitly connects to
- The Global facility grammar
- The static grammar
- The device user's personal grammar

Vocera always includes the static grammar, the grammar of the Global facility, and the device user's personal grammar while processing the voice commands. However, Vocera includes the dynamic grammar of only a single facility, not the grammars of each facility, while processing the command.

For example, suppose the Central Pacific Resort deployment has two facilities—Carmel and Monterey—in addition to the Global facility. If a device user in Carmel issues the command, “Call Adda Turner”, Vocera uses the following grammars to process it:

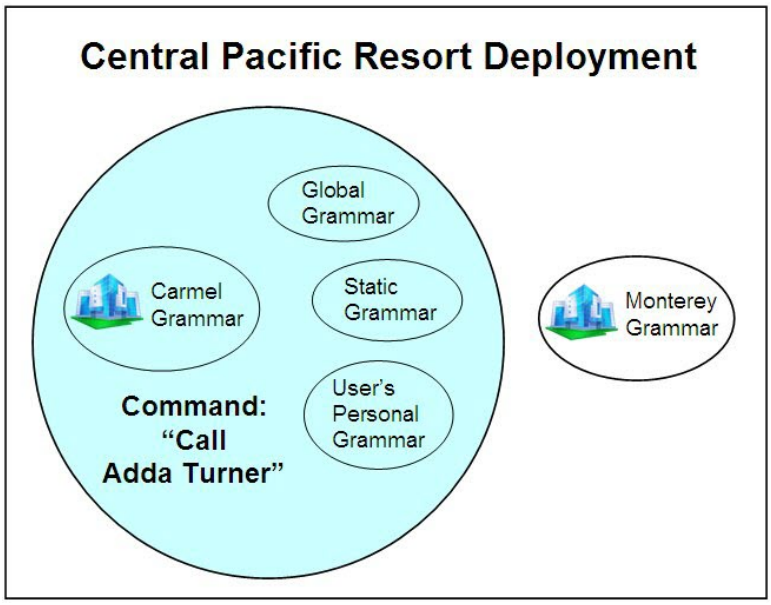


Figure 7: Grammars used at the Carmel facility

Contacting a device user at a remote facility is a two-step process. For example, suppose the Carmel user in the previous example wants to call Adda Turner, but Adda's home facility 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 facility—the current facility 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 facility, as shown in the following illustration:

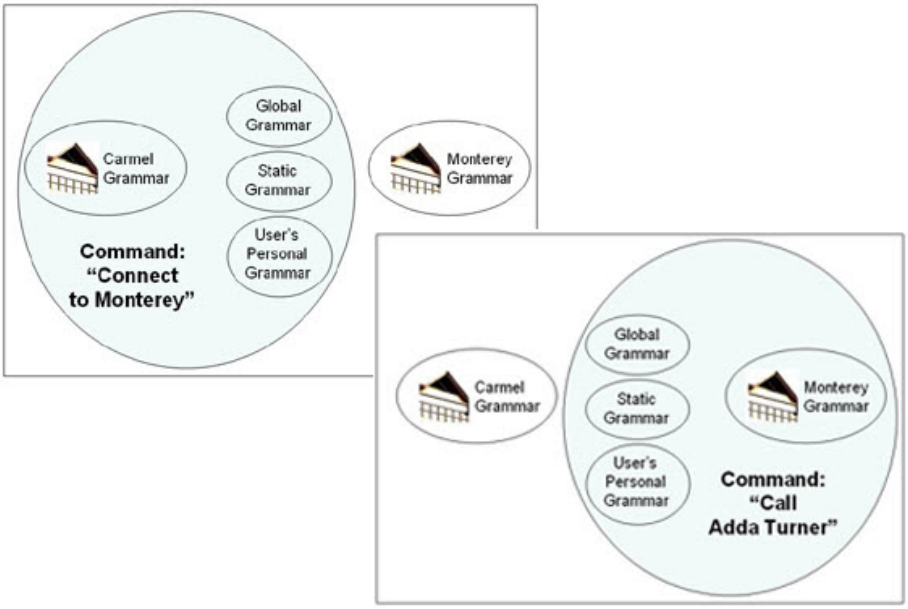


Figure 8: Grammars used after connecting to the Monterey facility

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 facility is not sharing a telephony server, Vocera searches the Global facility grammar and the grammar of the telephony server's facility.
- If the facility is sharing a telephony server and the caller spoke a response, Vocera searches the combined grammars of the Global facility and any facilities associated with the line that the call arrived on.
- If the facility is sharing a telephony server and the caller entered a touch-tone response, Vocera searches the combined databases of the Global facility and each facility that shares the telephony server.

See the Working with Multiple Facilities (in Telephony guide) for more 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 facility is the total number of names in the dynamic grammar of that facility. This count appears in the **Spoken Name Count** field under Voice section of the Add/Edit Facility page.
- The spoken name count for the system is the total number of names in the dynamic grammars of all the facilities 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 misrecognized speech increases. A large recognition space is more likely to contain similar sounding names.

Intelligent Command Backoff

Learn to use the Intelligent Command Backoff mechanism.

Intelligent Command Backoff is a mechanism to help improve accuracy in speech recognition. The backoff strategy enhances the user experience with Vocera voice commands. It offers additional help to users and significantly reduces the overall user frustration. This feature is typically useful if your organization has a big database of users and groups. Command Backoff is enabled by default, and no additional configuration is required.

Command Backoff triggers on when the Vocera Genie fails to recognize the names of recipients (individual or group) that a user uses with some commonly used voice commands, such as Call, Broadcast to, Add Me to, Record a Message for, etc.

For example, when you say the voice command, Call Mariah Carey from your badge, and Genie fails to recognize the receiver's name. You hear the following response, "I didn't understand."

Instead of repeating the "I didn't understand" messages, the command backoff strategy initiates after two consecutive failed attempts (i.e., after you hear two "I didn't understand" messages) to assist the user. It first asks if you are calling a user or a group, and then it asks you to say or spell the name of the user or group. Once you say or spell out the user or group's name, Genie recognizes the call recipient and proceeds with the command.

The following diagram describes the Call Command Backoff flow that Vocera voice prompt follows when a user tries to place a Call. If Vocera Genie fails to recognize the recipient's name during the first few attempts, the backoff feature prompts the user to say or spell the name of the User or the Group that they like to call.

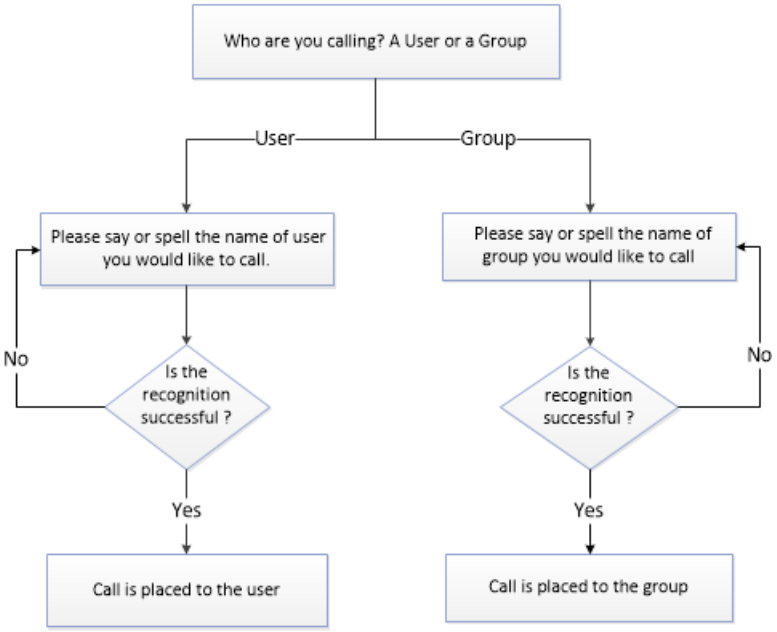


Figure 9: Backoff Flow for Call Command

Similarly, when you say the command:

- "Broadcast to *<group name>*" , and Genie fails to recognize the group name. After two consecutive failed attempts, the following message is played, "say or spell the name of the broadcast group".
- "Add me to *<group name>*" , and Genie fails to recognize the group name. After two consecutive failed attempts, Genie plays the following message, "say or spell the name of the group that you would like to be added to".
- "Record a message for *<user name>*", and Genie fails to recognize the recipient's name. After two consecutive failed attempts, Genie plays the following message," who are you trying to send a message to, "User" or "Group"?"

It is possible that Genie may fail to recognize a voice command that a user says even before attempting to recognize the recipient's name or a group's name. In such situations, after two consecutive attempts to recognize the command, the following message is played to assist the user: "say one of Call, Broadcast, Add me to group, or Send message to". Vocera Genie offers these command choices to help the user choose the correct command name.

Offer to Learn a Name

Train Genie to learn a caller's name

Vocera voice prompt offers an interactive way to learn the name of the most frequently called user if you spell out the user's name with the Call command. Vocera Genie plays a prompt offering to learn the name of the user that you called by spelling at the time of your next login. You can choose to accept this offer by saying, "yes" or decline the offer by saying, "no." When you accept the offer, Genie asks you to say the user's name three times after each tone sound. After this, the system saves the name of the user in the database.

For example, if you are calling a user named Emily and you say the command, Call "E M I L Y R O S E" (by spelling out the recipient's name). The system checks if this name exists in the database. If the name is not found, Genie takes you through the, "Learn a name" command flow.

At your next login, you hear the prompt; “You called Emily Rose by spelling, do you want to learn this name?” Say “Yes” to accept the offer. As soon as you accept the offer, Genie plays the prompt; “You may learn name for user Emily Rose, say the name each time you hear the tone”. Say the username after each tone sound, and at the end of the third tone, Genie says, “Okay, I got it” as a confirmation to have learned the username.

The offer to learn a name feature is available as a default. If you choose to decline the offer for three consecutive times, the Voice prompt will no longer offer to learn the user's name.

Note: This prompt is not played for VCS clients.

Learn a name offer is valid under the following conditions:

- If the call recipient's name is not in the system
- If you spell out the recipient's name with the Call command
- Learn a name offer is limited to learn only one user's name at each login
- If you declined the offer (by saying “No”) the first time Genie offers to learn this user's name, then Genie will play the prompt two more times after each consecutive logins
- If you declined the offer to learn a name for three consecutive times, the prompt is no longer played
- If there are more than one usernames to learn, the username with maximum number of call frequency takes precedence
- If there are two users with same number of call frequency, then Genie offers to learn the name for the latest call record

Groups

Groups provide a way to organize a collection of users and communicate with them at once.

Groups are assigned a set of voice permissions that group members (users) can use to perform tasks related to voice call flows and related features.

Groups do not have the ability to implement the mandatory access control mechanism for group members unless a Group is assigned a Role with a set of access control policies. To understand the relationship between group, roles, and policies and how they work together, see Understanding Groups, Roles, and Policies on page 168.

You can use the Vocera Platform Web Console to create and manage your groups.

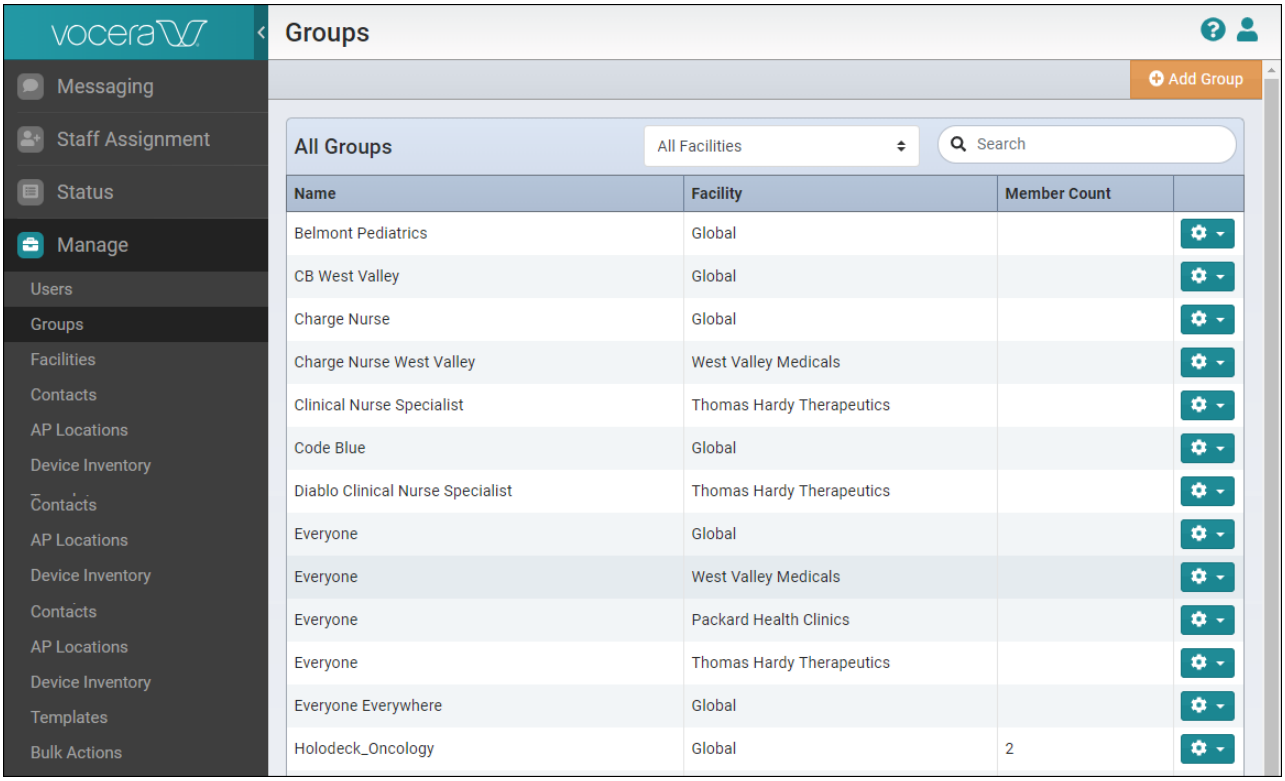
For example, oncologists who work at a facility named West Valley Medicals can belong to a group called Oncology.

Group members can belong to different facilities. For example, you can create an Oncology group with members from the West Valley Medicals facility, the East Palo Alto facility, and the Old San Francisco facility. For situations like this, you can assign the Oncology group to the Global facility to indicate that its members span multiple facilities.

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

The Groups page in the Vocera Platform Web Console allows you to add, edit, or delete a group. In addition to that, you can also assign group types to groups in your system and organize the group members for voice call flows and other related features.

To view all the groups in your system, select **Groups** in **Manage** section of the navigation bar. The Groups page displays with a list of Groups in alphabetical order.



Understanding Group Properties

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 notify or address multiple users at once (“Send a message to Nurses Assistants”), or to call someone who fits a specific role (“Call a salesperson”), 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.
- Membership properties define the set of users who are members in a group and the order in which Vocera routes calls to them when round-robin scheduling option is specified.
- Group Type properties determine whether a group is used as a department or a subdepartment, and optionally specify a telephony PIN or Cost Center ID for accounting purposes.
- Roles properties determine which roles are assigned to a group. Roles are directly linked to a policy with one or more policy items, and policy items are permissions to control user access. See Understanding Groups, Roles, and Policies for more information.
- Call Forwarding properties determine the flow of calls from one group to another, potentially through your entire organization.
- Voice Permissions determine the ability of users to issue certain voice commands or perform specific operations.
- 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.
- Conference properties determine which users are in an instant “push-to-talk” conference that simulates the behavior of a walkie-talkie.
- Emergency Broadcast properties determine which group members receive an emergency broadcast message in the event of an emergency.

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 voice 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 inherit the permissions that you specify for Marketing unless you revoke 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.

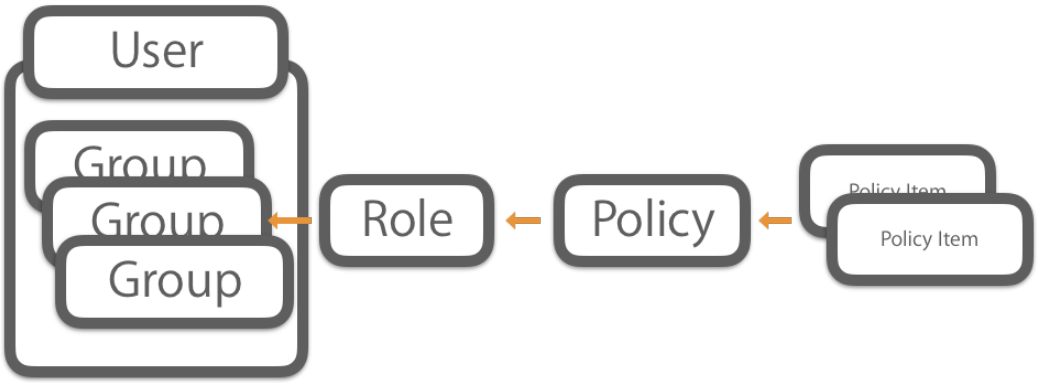
Understanding Groups, Roles, and Policies

Groups, roles, and policies are ways to control who can access the Vocera system and the actions they can perform.

System administrators can establish groups, roles, and policies to manage the system efficiently.

Group is a collection of users with a given set of voice permissions assigned to them. A role is a collection of policies, and a user effectively inherits the policies when assigned a role. The individual policies that we assign to a role are called policy items, and a set of policy items are defined in a policy. Policies are established to govern and manage the system.

The following figure shows the association between user, group, role, policies.



Designating Group Types

Assigning a group type to a group allows organizing multiple groups and group memberships for voice call flows and other related voice features.

You can designate a group as an ordinary group, a department group, or a subdepartment group in the Vocera Platform Web Console. You can designate a group as an ordinary group, a department group, or a subdepartment group using the Group Type field in the console when you create a group. All groups that are not designated as a department or subdepartment in the Group Type field in the Add New Group page are ordinary groups by default.

Department Group

A department group, also known as 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.

Sub-department Group

A **Subdepartment** group type is a subgroup of a **Department** group. Members of a subdepartment are also assigned to the parent department group for department specific calling feature.

Subdepartment 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 subdepartment should have their **Group Type** field set to subdepartment. You can create multiple levels of nested subdepartment groups within a department.

A subdepartment must be a member of a single parent department. You cannot make the same subdepartment group as a member of multiple departments.

Default Groups

Vocera automatically creates and maintains the default **Everyone** group and the **Everyone Everywhere** group.

The system automatically creates and maintains a special group called **Everyone** group when you add a new facility. When you create or delete a user, the system adds or removes that user from the appropriate **Everyone** group automatically. By default, the **Groups** page in the **Manage** section of the Web Console displays an **Everyone** group for each of your facilities.

For a single-facility deployment, Vocera maintains the group for the Global facility. For a multi-facility deployment, Vocera maintains a separate group for each physical facility as well as an **Everyone** group for the Global facility.

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

The order of names in a group affects the group scheduling properties, which determine how calls are routed.

Tip: Because Vocera automatically adds new users to the end of the **Everyone** group, you may want to rearrange this order to optimize scheduling manually.

The **Everyone** group determines the default set of permissions for the users at that facility.

The “Everyone Everywhere” Group

After you complete your installation and upgrade, the system also creates an **Everyone Everywhere** group. Similar to an **Everyone** group, the system automatically maintains the membership for the **Everyone Everywhere** group, but you can specify all other properties for this group. There is only one **Everyone Everywhere** group, and it is associated with the Global facility.

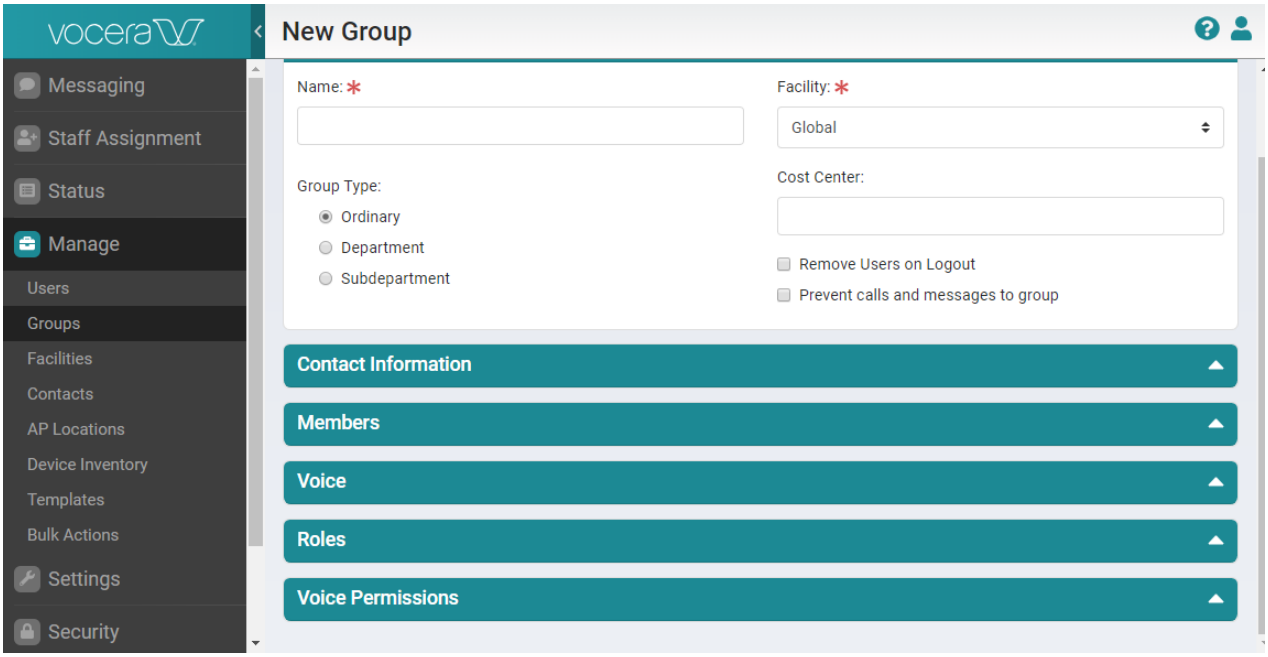
Each **Everyone** group is a member of **Everyone Everywhere**.

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

Adding a Group

You can add a group to your list of groups in Web Console.

1. Navigate to **Groups** in the **Manage** section, and click **Add Group**. The New Group page displays.



The New Group page has six sections:

- General
- Contact Information
- Members
- Voice
- Roles
- Voice Permissions

Tip: You can click the drop down arrow at the right hand side of each section to expand or collapse these sections.

2. In the General section, complete the fields listed in the table below. An asterisk * indicates that a value must be entered for this field.

Field	Description
Name *	The name of the group.
Facility *	The name of the facility for the new group. If you have not defined any facility, or if you do not want to specify a facility for the new group, use the default **Global** value for this group.

Field	Description
Group Type	Select one of the following three types: • **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 voice 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. **Note:** The **Department** group type should not be confused with the physical **Department** associated with a Facility. Adding a voice department group type will not link it with the Facility for this group. 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.
Cost Center	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.
Remove Users on Logout	Select this checkbox to specify that membership in the group is temporary. When you select this checkbox, 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 facility 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** checkbox in the Preferences section of **System Configuration** in **Settings** section of the Web Console 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.
Prevent calls and messages to group	Select this checkbox to prevent calls and messages from reaching the members of a specified group.

3. In the Contact Information section, optionally complete the fields listed in the table below.

Field	Description
Vocera Phone	The phone number provided for the new group with Vocera Vina.
Pager	The pager number for the new group.
Emergency Broadcast Group	The name of the group that receives emergency broadcasts for a functional group. Click **Find Group** to find this group in the list of existing groups. **Note:** A silent emergency broadcast is configured at the facility level only and will apply to all emergency groups for the entire facility.

4. In the Members section, click **Add Members** to add members to the new group. In the Add Members dialog box that appears, click on the names of the members that you want to add. Click **Previous** and **Next** or the arrow keys to page through the list of members as needed. Click **Done** when finished.
5. In the Voice section, specify Vocera Platform properties for voice access to the new group, as defined in the tables below.

   Scheduling Options:

Field	Description
Sequential	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.
Round Robin	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.

Forwarding:

Field	Description
No Forwarding	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	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 User, Group, or Contact	Transfers the call to a particular badge user, group, or contact entry when no members of the original group can take the call. See Forwarding Calls to Users, Groups, or Contacts for more information. When you forward to a group, the forwarding settings of individual group members are ignored.
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	Enables on-call group members to receive calls when they are off-network.
Forward When	This field appears only when you select the **Forward to an Off-network Group Member** field. Choose one of the following: • **All** — forward all incoming calls. • **Unanswered**— forward only calls that are not answered.

Enable Group Voicemail — Permits users to leave voicemail recordings for the group. The group voicemail option is enabled by default. Users can send voicemail only to the groups in which they are members.

Forwarding Condition:

Field	Description
Forward On Broadcast to Number	Forward every call that comes in to the group, without notifying group members.
Forward On Conference to Number	Forward only calls that are not answered by any member of the group.

Fields in the column on the right:

Field	Maximum Length	Description
Member Name-Singular	50	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	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	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."
PIN for Long Distance Calls	50	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.
Cross Facility Option - Receive Offsite Calls	n/a	Select this checkbox to permit calls to the group to be received by members who are currently at a different facility from the caller. If your Vocera system has only one facility, this option does not apply. If you don't want members to receive calls to the group when they are currently at a different facility from the caller (if the group's facility is Global) or at a different facility from the group (if the group's facility is not Global), clear this checkbox.
Cross Facility Option - Receive Offsite Broadcast	n/a	Select this checkbox to permit broadcasts to the group to be received by members who are currently at a different facility from the person who initiated the broadcast. If your Vocera system has only one facility, this option does not apply. If you don't want members to receive broadcasts to the group when they are currently at a different facility from the caller (if the group's facility is Global) or at a different facility from the group (if the group's facility is not Global), clear this checkbox.

In the Conference Users section, you can maintain the list of users who are in the conference with the same name as the group. To add to this list, click **Add Conference Users**.

6. In the Roles section, click **Add Role** to associate a role with this group. Roles control what capabilities of the Vocera Platform Web Console are available to this group. See Roles on page 417 for more information on roles.

   In the Add Role dialog box that appears, select a role from the drop-down list and click **Done**. Repeat this step to add additional roles for this group.
7. In the **Voice Permissions** section, specify Vocera Platform permissions for the new group, see Granting Group Voice Permissions for more information.
8. Select one of the following to close the dialog:
   - **Save** — to add the new group to the system.
   - **Cancel** — to return to the Groups page.

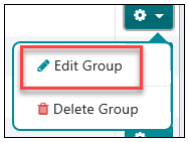
Editing a Group

You can edit the information for any existing group.

1. Click **Groups** in the **Manage** section.
   All groups for the selected Facility are displayed.
2. Locate the Group that you want to edit.
3. Choose one of the following:
   - Click on the name of the group that you want to edit to display the Edit Group page.

- Click the **Options** button in the far right of this group.

1. Select **Edit Group** from the dropdown menu in the **Options** button.



2. The Edit Group page displays.

4. Edit the group information as necessary. See Adding a Group on page 170 for a list of the group fields.
5. Choose one of the following to close the dialog:
   - **Save** — to update the group configuration changes.
   - **Cancel** — to return to the Groups page.
   - **Delete Group** — to remove the group from the system permanently.

Granting Voice Permissions

The Voice Permissions section of the Edit Group page lets you control the ability of users to access or use specific voice features.

To grant voice permissions:

1. Click on the **Group** for which you want to enable voice permissions.
   The Edit Group page appears with fields to edit.
2. Scroll down to **Voice Permissions** section and click the dropdown arrow to display all the 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: 1. click the **Find Group** button next to **Group of users permitted to manage this group** to display the Find a Group dialog box. 2. Use the **Previous** and **Next** buttons to page through the list of groups displayed in this dialog box. 3. Choose a group that has management privileges, and then click **Select Group** 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.
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: 1. click the **Find Group** button next to **Group of users permitted to add themselves to this group** to display the Find a Group dialog box. 2. Use the **Previous** and **Next** buttons to page through the list of groups displayed in this dialog box. 3. Choose a group that has this permission, and then click **Select Group**. For example, you may want to assign members of the Nurses group the permission to add themselves to a group called On Duty.
Group of users permitted to manage group's devices	To let members of an existing group manage the Vocera devices owned by this group: 1. click the **Find Group** button next to **Group of users permitted to manage group's devices** to display the Find a Group dialog box. 2. Use the **Previous** and **Next** buttons to page through the list of groups displayed in this dialog box. 3. Choose a group, and then click **Select Group**. 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.

Field	Description
Permission	Select an item in the Permission list to grant permissions for a selected group. Select the options button: Then, select one of the following options: • Select **Grant** to grant members in the group the authority to perform the selected action. • Select **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. • Select **Clear** to reset the permission for the selected action.

3. Select one of the following to close the dialog:
   - **Save** — to save the group permissions.
   - **Cancel** — to return to the Groups page.

Voice Permissions Reference

As a system administrator, you can grant or revoke the following voice permissions to a specific group in the Vocera Platform Web Console.

System Administrator Permissions

System Admin Permission	Description
Perform Voice Administration	Gives a group full administrative privileges in the Web 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 on the device This permission overrides any revoked permissions inherited by membership in other groups, except the revoked Perform Voice Service Administration permission itself.
Record Name Prompts for Another User	Grants permission to record name prompts for other users, as well as groups and contacts entries. Name prompts improve the usability of the Vocera system; the Genie plays these name prompts when necessary, instead of synthesizing speech.
Can Login as Another User	Grants permission to login as another user and automatically grants permissions to the user's groups and permissions, except for the ones that require: • Authentication to Log In • Authentication to Play Messages on the device

Call Permissions

Several of the call permissions require Telephony integration.

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 Numbers	Grants permission to place calls to phone numbers that are not in toll-free calling areas. 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.
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 My Profile 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 My Profile 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 My Profile 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 My Profile 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 facility'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 Guidefor 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 Guidefor more information about urgent calls.
Call Users at Other Facilities	Grants permission to contact a user whose current facility is different than the current facility of the caller.
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

Call Permission	Description
	permission and use the Web Console to remove the user from a conference.
Send Messages to Everyone	Grants permission to send a message to all users in your facility'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.

Security Permissions

Administrators can set up security permissions to authenticate users in group through a voice PIN number. Users can record a 5 digit voice PIN to secure their voice messages.

PIN Permission	Description
Require Authentication to Log In	Grants permission to enable voice PIN authentication for user at the time of logging-in to the Vocera systems. When this permission is granted, users must enter a 5 digit voice PIN to log in. **Note:** Administrators cannot login as another user, if the user has a voice PIN set up for login.
Require Authentication to Play Messages	Grants permission to enable voice PIN authentication to listen to messages. When this permission is granted, users must enter a 5 digit PIN to listen to their voice messages. **Note:** Administrators cannot play the voice messages when they login as another, if the user has a voice PIN set up for playing messages.
Record Your Voice Pin	Grants permission to record a voice PIN authentication number. When this permission is granted, users can record a 5 digit voice PIN through voice commands.
Erase Your Voice Pin	Grants permission to delete a voice PIN number. When this permission is granted, users can erase their previously recorded voice PIN using the voice command.
Erase Voice Pin of Another User	Grants permission to delete the voice PIN for another user. When this permission is granted, a user (typically the system administrator) can erase the voice PIN set up by another user.

Special Permissions

Certain special voice features requires the administrator to grant special permissions to the user.

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 Access Point Locations for more information.
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 Genie from Phone 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.
Code Lavender	Grants permission to start (live broadcast) or schedule a Code Lavender call for a specific group. Members who schedule a Code Lavender event can cancel a scheduled Code Lavender event.
Code Lavender for Everyone	Grants permission to start (live broadcast) or schedule a Code Lavender call for **Everyone** group and **Everyone Everywhere** group. Members who schedule a Code Lavender event can cancel a scheduled Code Lavender event.
Add/Edit/Delete Reminders	Grants permission to add, edit, or delete reminders for members of a specific group.
Add/Edit/Delete Reminders to Everyone	Grants permission to add, edit, or delete reminders for **Everyone** group and **Everyone Everywhere** group.

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 contacts 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 calls are forwarded according to the options she specifies through voice commands or the My Profile > Call Forwarding settings.

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.

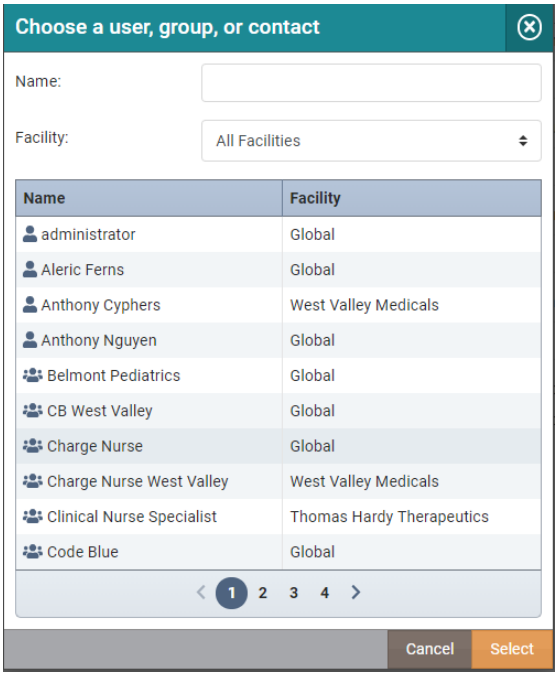
If this option is selected, Vocera sends the call to a device that is not in-network or off-campus using the forwarding behavior configured in the My Profile > Call Forwarding settings for that user.

Forwarding Calls to Users, Groups, or Contacts

Forward calls to another user, a group, or a contact in the system.

Forwarding calls is helpful when you cannot answer a call for any reason, or when you block all calls or put your device in Do Not Disturb mode; your caller is usually prompted to leave a message.

1. Click **Groups** in the **Manage** section to display a list of Groups.
2. Click on the Group that you want to edit for the forwarding settings.
   The Edit Group page displays
3. Scroll down to the **Voice** section in the Edit Group page.
4. Select **Forward to User, Group, or Contact**.
5. Click the **Choose** button to display the Choose a user, group, or contact dialog box with a list of all the choices available in the system.



If you know the name of user, group,or contact that you want to choose to forward the calls, you can enter the name in Name field search bar.on the left of the Choose button and click **Choose**.

You can enter the name in the **Name** Field to search for a user, group, or contact that you want search in the system. You can also use the **Facility** field to toggle between multiple facilities available in your system and refine your search.

6. Select one of the following to close the dialog:
   - **Select** — to save the selected user, group, or contact as your choice for forwarding calls.
   - **Cancel** — to return to the Edit Group page.

About Emergency Broadcast

Emergency broadcast is a scalable emergency notification feature that you can set at the facility or group level in the Vocera Platform Web Console.

Emergency broadcasts are initiated on the Vocera device when you click the Call button on your Vocera device 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.

Emergency Broadcast at the Facility Level

You can designate an existing group in a facility as the emergency broadcast target group, or add specific members to a group utilizing it as the emergency broadcast target. Each facility can have only one emergency broadcast target group.

Emergency Broadcast 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 facility level emergency target group (if configured). In addition, If an emergency broadcast group is not designated at the facility or group level, the default behavior is to use the emergency broadcast target group set at the Global facility.

If the emergency broadcast initiator triggers a facility-level emergency, it will preempt or cut through any members already receiving a group emergency broadcast.

You cannot designate the **Everyone** and **Everyone Everywhere** group as an emergency broadcast group.

Configuring Code Lavender

Vocera users can schedule a Code Lavender® event or start a live Code Lavender broadcast event for group members to bring comfort and spiritual support to employees and physicians during times of high stress.

Code Lavender® is considered as an integrative medicine service and a vital tool to ensure that individuals are able to continue after being presented with a difficult case, diagnosis, or loss. Hospital staff, patients, and family members often fall victim to fatigue, despair, and generally negative feelings that may impact all attempts of healing. A Code Lavender event ensures that hospital employees, patients, and patient families feel that they have the mental and emotional strength and energy to cope with challenging situations.

Code Lavender is recommended after one of the following events:
- Death of a patient
- Major trauma
- When facing an ethical dilemma in patient care
- Difficult encounters with a patient or patient's family
- Difficult encounters within the team
- During times of high stress or emotional distress

During a Code Lavender event, a rapid response team of specialists is called upon to resuscitate the emotional, spiritual, and physical well-being of staff and physicians following an adverse event.

Vocera Code Lavender feature allows group members to start a live broadcast call or schedule a reminder for a Code Lavender event to begin at a later time. All recipients of the Code Lavender call are notified with a voice message, email (if configured), and a voice reminder. The badge halo turns to purple color for 5 minutes indicating the start of the Code Lavender event.

Note: The default duration for which the purple halo glows on the badge is 5 minutes. Administrators can modify the `SysCodeLavenderHaloDuration` property value in the `properties.txt` file (in the `\vocera\server\` directory) to change the default duration and configure a new value.

Vocera recommends calling Customer Support if you plan to manually update the `properties.txt` file.

Administrators can designate an existing group as the Code Lavender group, or add specific members to a group utilizing it as the Code Lavender Broadcast group. Members of this group and the target group will receive Code Lavender broadcast calls as well as scheduled event reminders.

For example, you may have a group named Charge Nurses with Code Lavender permissions, a second group named CL Participants that you can designate as Code Lavender Broadcast Group, and the third group as your target group, such as Palliative Care.

Any member who is part of the Charge Nurses group can initiate a Code Lavender broadcast call or schedule a reminder for a target group named Palliative Care. When a member from Charge Nurses group says the command, "Start Code Lavender for Palliative Care", all members of CL Participants group and Palliative Care group receive a Code Lavender broadcast call. Therefore, in a Code Lavender call :

- Code Lavender Callers – Anyone with Code Lavender permissions (members of Charge Nurses group).
- Code Lavender Receivers – Members of Code Lavender broadcast group and the target group (members of both CL Participants and Palliative Care).

Code Lavender is disabled by default. Administrators can enable Code Lavender for a specific Facility and grant the required special permissions, see the "Group Voice Permissions" section in the Vocera Platform Administration Guide. For information on enabling Code Lavender for a specific Facility, see the "Enabling Code Lavender" section in the Vocera Platform Administration Guide.

Broadcast a Live Code Lavender Event

In a live broadcast Code Lavender event, a call initiator from a designated Code Lavender group can start a broadcast call saying, "start a code lavender for <group name>" voice command. All Code Lavender recipients immediately receive a broadcast call alert with a voice message from the caller. When the recipients press the Call button on their badge (to receive the call), the Vocera badge halo turns to purple color and remains in this state for 5 minutes. This indicates the start of a Code Lavender event.

Call initiator and recipients can press the Call button to cancel out of the Code Lavender broadcast call, the badge halo may continue to glow a purple halo for the 5 minutes.

If a recipient has call forwarding set on another phone, the Code Lavender broadcast call is forwarded to this phone. on the phone. If a recipient is offline or off network, they will not receive the Code Lavender broadcast call.

Scheduled Code Lavender Event

In a scheduled Code Lavender event, a call initiator from a designated Code Lavender group can schedule a Code Lavender event for a later time by saying, “schedule a code lavender for <group name>” voice command. When you schedule a Code Lavender event, system prompts you to set a time and record a voice message for the Code Lavender event. Immediately after the event is scheduled, all the recipients receive a message alert, email notification, and a Vocera prompt to listen to the Code Lavender voice message and reminder.

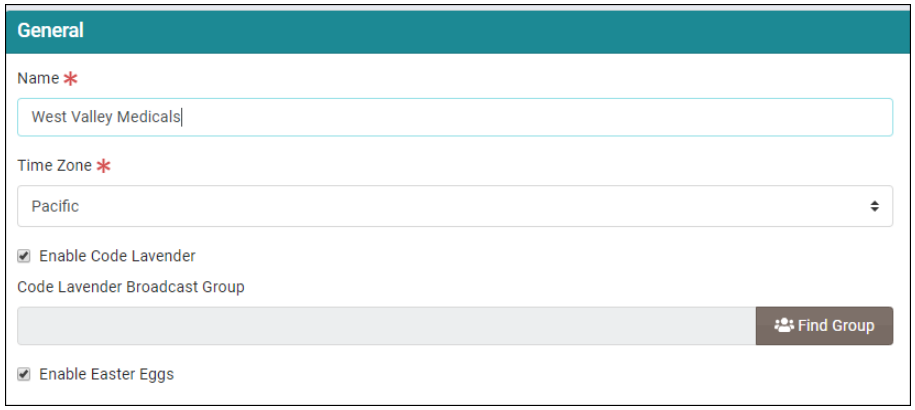
For scheduled Code Lavender events, a reminder is played 15 minutes before the scheduled time. The Vocera badge halo of all participating group members turns to purple color for 5 minutes to indicate the beginning of the Code Lavender event. If a recipient is offline or off network, the Code Lavender reminder is sent to their voicemail.

Enabling Code Lavender

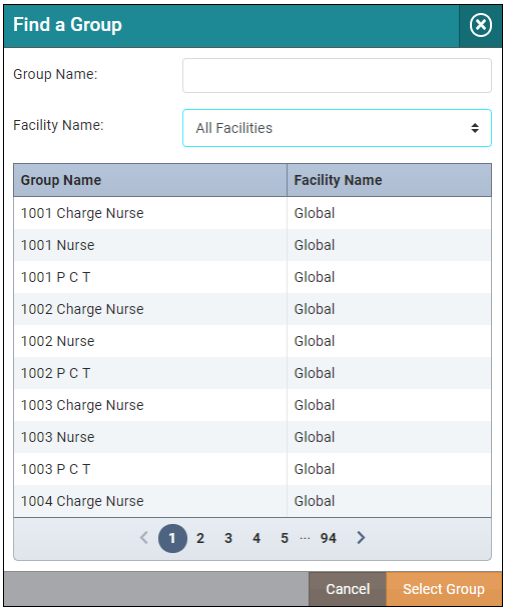
You can enable Code Lavender feature for a Facility in your system.

1. Click **Facilities** in the **Manage** section.
2. Click **Add Facility** button to add a new facility, or choose an existing Facility from the list and click **Edit Facility**.

   Tip: If you have a long list of facilities in your system, the **Search** bar can help you find a facility name quickly. As you type a name, the search finds the closest match to the facility name that you entered.
3. Select the **Enable Code Lavender** checkbox in the General section of the Edit Facility page or New Facility page (if you are adding a new facility).
   As soon as you select the Enable Code Lavender checkbox, the system will display an an option to choose a **Code Lavender Broadcast Group**.



4. Click **Find Group** to choose a **Code Lavender Broadcast Group** from the Find a Group dialog box.



5. Click **Save**.

After the Code Lavender feature is enabled, you can initiate a Code Lavender broadcast call or schedule a Code Lavender call on your device, see the supported Device User Guide on the Vocera Devices page for more information.

Using Voice PIN Authentication

Voice PIN authentication allows badge users to record a 5-digit Personal Identification Number (PIN) to securely login or access your voice messages.

Voice PIN authentication adds an extra layer of security and convenience to Vocera administrators and badge users by limiting access to the Vocera system on the basis of a pre-recorded voice PIN. This ensures that all unauthorized or fraudulent users are prevented from using an authorized badge user's name to login and issue commands. A voice PIN functions like a secure voice command or password that prevents unauthorized users from playing voice messages on a badge that was inadvertently left logged in by a user.

Badge users can use the voice PIN commands to record or erase their PINs, see Vocera Voice Commands Reference Guide for additional information.

When voice PIN authentication is enabled, badge users are required to record a pre-determined PIN number of their choice to login to the Vocera system or to access their voice messages. By default Vocera allows badge user to record a 5-digit PIN. Badge users can choose any 5 numbers between the range of 0 to 9 to create a voice PIN.

Voice PIN authentication is disabled by default. System administrator must enable the required security permissions to allow authorized users to record their voice PINs, see the security permissions mentioned in Voice Permissions Reference section in the Vocera Platform Administration Guide.

A user can initiate a recording session by issuing the “Record a voice PIN” command through their badge. When a user is enabled for voice PIN authentication and records a PIN, the system challenges the user to say the PIN each time they log in. If the correct PIN is entered, the user is permitted to login or play voice messages. When system fails to match the PIN, user is denied login and asked to recite the correct PIN.

System administrator can enable the voice PIN authentication in **Groups** in the **Manage** section of the Web Console, see the Enabling Voice PIN Authentication section for more information.

Enabling Voice PIN Authentication

You can login to the Web Console and enable Voice PIN authentication for group members.

To enable voice PIN authentication, follow these steps:

1. Click **Groups** in the **Manage** section to display a list of Groups available in your system.
2. Locate and click the Group that requires voice PIN authentication.
   Edit Group page appears with fields that you can modify.
3. Scroll down to the **Voice Permissions** section
4. Locate the following Voice PIN permissions under the **Permissions** section.
   - **Record Your PIN** — allows a user to record a voice PIN.
   - **Erase Your PIN** — allows a user to erase a voice PIN.
   - **Erase PIN of Another User** — allows a user to erase the voice PIN for another user. You typically assign this permission to an administrator.
5. Click the **Options** button in the far right of each permission and select the **Grant** checkbox from the dropdown list to enable each permission.
6. Click **Save** to update the group permission, or click **Cancel** to return to the Groups page.

Group Managers and Device Managers

Designated group managers can change and review group capabilities. Similarly, designated group device managers can manage device related permissions for the groups they manage.

Group managers can view all groups in the Web Console and grant them the View Users and Groups permission. Otherwise, they will only be able to view groups that they manage on those pages. You can have members of different group manage a specific 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.

Note: Group managers do not have system administration permission. Only a system administrator can create a group, delete it, or assign permissions to it.

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 such as alternate spoken names, 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.

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 supported Vocera Device User Guide for your device on the Vocera Devices page for more information.

Device Managers

System administrators can designate members of a group as “device managers” to manage the devices owned by members of another 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.

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 device managers group does not require any additional permissions.

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

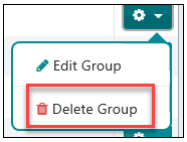
- View the Device Status Monitor to monitor the status of devices currently connected to the network.
- View the Devices page for groups whose devices they manage.
- Modify Owner, Facility, Status, MAC Address, Label, Tracking Date, Is Shared, and Notes fields for a device.

Deleting a Group

Barring the default Everyone group and the Everyone Everywhere group, you can delete an existing group from the Web Console.

1. Navigate to **Groups** from the **Manage** section to locate the group that you want to delete.
2. Click the **Options** button in the far right of the group that you want to delete.

3. Select **Delete Group**from the dropdown menu in the **Options** button.

   The system displays a confirmation message to confirm if you really want to delete the selected group
4. Choose one of the following to close the dialog:
   - **Yes** — to confirm the delete action.
   - **No** — to cancel the delete action and return to the Groups page.

Facilities

Facilities are names of hospitals or other facilities that are associated with your Vocera Platform.

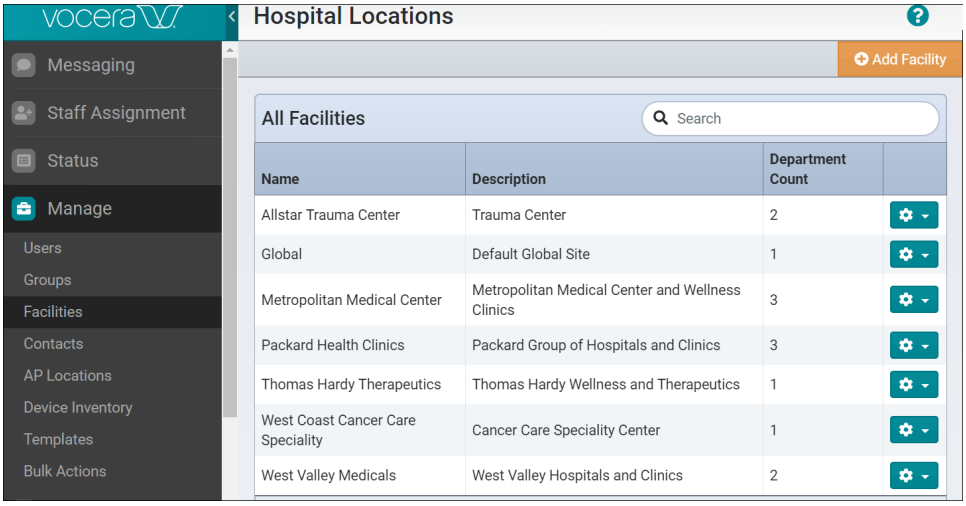
A hospital may have multiple facilities or locations in their network. A facility can be in multiple locations, and users can work with the departments, rooms, and beds associated with a location. See About Departments, Rooms, and Beds for more information.

Once created, facilities allow staff assignment to the specified beds via the **Manage Functional Roles** workflow provided in the Vocera Platform solution. For example, many beds on a Medical-Surgery department may require respiratory monitoring. You can organize these beds into a virtual location in the system, allowing the respiratory therapists to focus on the specified patients easily.

A hospital location is a way to organize patient locations for staff assignment purposes. Facilities do not need to change this information often, and an authorized IT Administrator makes these changes.

Note: Only the Administrator role can manage Hospital Locations; contact a System Administrator for assistance.

To view all the facilities in your system, select **Facilities** in **Manage** section. The Hospital Locations page appears, with a list of locations displayed in alphabetical order under the All Facilities header.



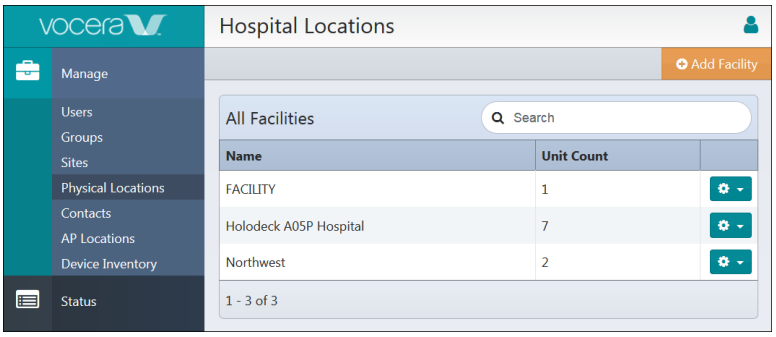
From the Hospital Locations screen, you can add, edit, or delete a facility.

Adding a Facility

You can add a new facility to the list of physical locations from the Vocera Platform Web Console.

1. Select **Facilities** in the **Manage** section.
   The Hospital Locations page displays.

2. Click the **Add Facility** button.



3. In the General section, click the cursor in the **Name** field and enter the name for your new facility.

4. Complete the fields listed in the table below. An asterisk * indicates that a value must be entered for this field.

Name	Maximum Length	Description
Name *	100	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.
Description	100	An optional abbreviation to represent this facility name.
Time Zone*	n/a	Use the **Time Zone** dropdown menu to select a time zone for the facility.
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 facility. You also set an emergency group for each functional group in your organization. For more information, see About Emergency Broadcast.
Enable Code Lavender	n/a	Check the **Enable Code Lavender** checkbox to enable Code Lavender for this facility. This option is off (unchecked) by default. For more information on configuring Code Lavender, see Configuring Code Lavender on page 180.
Enable Easter Eggs	n/a	Uncheck the **Enable Easter Eggs** checkbox to disable the Easter Eggs commands. This option is enabled (checked) by default. For more information on Easter Eggs, see Playing with Easter Eggs on page 201.

Name	Maximum Length	Description
Initiate Emergency Broadcast Silently	n/a	Specifies whether to initiate emergency broadcasts at this facility silently, that is, without playing a chime first. This option is available only if a group is specified in the **Emergency Broadcast Group** field at the facility and group. By default, the option is not selected, see Initiating Emergency Broadcast Silently for more information. **Note:** This field is not available for **Groups**. A silent emergency broadcast is configured at the **Facilities** level only and applies to all emergency groups for the entire facility including panic groups set per group.

If Voice Service is used, provide the following information.

Name	Maximum Length	Description
Cost Center	100	(Optional) Use the **Cost Center** field to specify a cost center for the facility.
Alternate Spoken Name	50	(Optional) Use the **Alternate Spoken Name** field to enable Vocera to recognize variations of the exact facility name. For example, if users commonly refer to a facility by a nickname or an acronym, enter that variation here.
Spoken Name Count	n/a	(Optional) The **Spoken Name Count** field displays the total number of names that you can use in a voice command for this facility. It includes the names of users, groups, facilities, contacts 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.

5. Select the **Enable Telephony Integration** checkbox to allow Vocera and your phone system to communicate with each other and configure the fields related to basic telephony information.

   When the **Enable Telephony Integration** checkbox is not selected, all telephony related fields are also disabled.

   You can clear the **Enable Telephony Integration** checkbox and click the **Save** button to disable telephony features for a facility. Vocera saves your telephony settings but disables communication to the PBX.

   a. Enter the **Telephony - Basic Information** for the following fields:

Name	Maximum Length	Description
Number of Lines	3 digits	Specify the number of lines you want to provision for each telephony service in the **Number of Lines** field. Enter either of the following values, whichever is smaller: • The number of lines supported by your license. • The number of lines provisioned by the PBX for a single telephony service. If you are configuring a high availability array, enter the number of lines available to a single telephony service, not the total number of lines available to all services. For example, if you have 2 Vocera SIP Telephony Gateway (VSTG) services and your license contains 48 lines, specify 24 in this field to give each service 24 lines for a total of 48. The number of lines that you provision for each telephony service is decremented from the number of lines in your license.
Local Area Code	3 digits	Enter the area code of the region in which the Voice Service is installed in the Local Area Code field.
Omit Area Code when Dialing Locally	n/a	Check the Omit Area Code field when dialing locally. If your PBX requires you to dial local calls without using the area code you can enable this option. By default, Vocera includes the area code in the dialing string, even when dialing a local number. Check this field if your PBX or locale requires you to omit the area code when dialing local calls.
Voice Hunt Group	n/a	Specify the area code and phone numbers of the DID lines or hunt group you set up for the Vocera system in the **Vocera Hunt Group Numbers** fields. There are two hunt group number fields: • **Guest Access** — This number is for guest access to the Vocera system. When callers dial the Guest Access number, they are allowed to place a call but are not identified to the called person. Because guest users are not authenticated, they can call other users, but they cannot issue voice commands. To use the **Guest Access** number with numeric pagers, enter an asterisk after the last digit of the phone number. When a user sends a numeric page, Vocera passes the value that you enter in this field to the pager and then passes the user's desk extension to the pager. Some pagers display the asterisk as a hyphen, separating the desk extension from the Vocera number. • **Direct Access** — This number is for specially licensed user access to the Vocera system. This field is used only if 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** phone number from their desk phone or cell phone.
Default Local Access Code	n/a	Specify the sequence of numbers you use to get an outside line. For example, a PBX might require you to dial a 0 or a 9 or an 8 to get an outside line. By default, Vocera prepends this access code to any number within the local area code.

Name	Maximum Length	Description
Default Long-Distance Access Code	n/a	Specify the sequence of numbers you enter before placing a long distance call. For example, a PBX system might require you to dial a 9 to get an outside line and then dial a 1 before a long-distance telephone number. In this situation, the Default Long-Distance Access Code is 91. By default, Vocera prepends this access code to any number that includes an area code that is not the local area code.
Company Voicemail Access Code	n/a	Use the Company Voicemail Access Code field to specify the sequence of numbers you use to access the company's voice mail system. A typical entry includes X, then the sequence of digits that you dial to get into the voicemail system from an internal phone, and possibly special dialing characters such as the * or # to indicate the end of the sequence.
SIP Settings	n/a	Specify the SIP settings: • **Call Signaling Address** — Enter the call signaling address for your IP PBX or VoIP gateway. For PBX failover support, enter a comma-separated list (up to 256 characters) of call signaling addresses for two or more PBXs or gateways in order of preference. Enter each call signaling address in this format: `IP_Address:Port` The `Port` is optional. If you do not specify a port, port 5060 (the default) is used. VSTG uses only one PBX or gateway at a time. If you specify multiple call signaling addresses, VSTG tries each PBX or gateway in the order specified and uses the first one that responds. If that PBX or gateway goes down, Vocera SIP Telephony Gateway switches to another one. The preference order of call signaling addresses is important. If the Vocera SIP Telephony Gateway is currently using the PBX for the second call signaling address, and then the PBX for the first call signaling address becomes active, Vocera SIP Telephony Gateway automatically switches to the first PBX. **Note:** The Vocera SIP Telephony Gateway uses the response to a SIP OPTIONS message to determine if the PBX or gateway is currently available. The OPTIONS message is sent every 30 seconds by default. For more information on configuring Vocera SIP Telephony Gateway to use an OPTIONS message for keep-alive, see Detecting the Connection to the IP PBX. If the PBX or gateway is not configured to support SIP OPTIONS, then entering a second call signaling address has no effect. In some situations, using TCP as the signaling transport protocol reduces the length of time required for the VSTG to recognize that the current PBX is down and move to the next PBX in the list. • **Call Party Number** — Enter the DID number, including the area code, of the Vocera trunk (the number of digits depends on the locale). Outgoing calls use this value as the caller ID. However, you can configure Vocera SIP Telephony Gateway to use caller information contained in the dial signal from the Voice Service as the caller ID.

b. Expand the **Telephony - Access Code Exceptions** section and click **Add Exceptions** to add an exception for the entire area code, a specific prefix, or for a range of numbers within an area code.

By default, numbers in the local area code use the Default Local Access Code, and all others use the Default Long-Distance Access Code. For more information on Telephony-Access Code Exceptions, see Access Code Exceptions more information.

c. Expand the **Telephony - Toll Exceptions** section and click **Add Exceptions** to add any exceptions for an entire area code, a specific prefix, or for a range of numbers within an area code.

   You must add an exception to this list in either of the following situations:

   - When a number or range of numbers in your local area code is a toll call.
   - When a number or range of numbers outside your area code is a toll-free call.

   For more information on Toll Exception configuration, see Toll Exceptions.

d. Expand the **Telephony -DID Information** section and click **Add DID** to specify the range of Direct Inward Dialing (DID) extensions that are available for use by Vocera users.

   If your PBX administrator provides a hunt group number as part of the DID range, do not include it in the range of DID extensions you specify here. The extensions on this page are for use by users only.

   For more information on DID configuration, see Direct Inward Dialing.

e. Specify Telephony Personal Identification Numbers (PINs) in **Telephony -PINs** section.

   - **PIN for Long Distance Calls** — Enter a PIN for a facility. If a telephony PIN is not specified in the user's profile, and the user does not belong to a group that has a PIN, then the facility PIN is used. The facility-level telephony PIN is used for long distance numbers specified in Contacts. It is also used for group forwarding numbers, unless the group is a department group with a PIN number specified, in which case the department group PIN is used.
   - **PIN Template**— Specify a template for adding a PIN to a dialing sequence. A PIN template can include digits, special characters, and PIN macros.

     When a dialing sequence includes a PIN, this value defines the format that the Vocera system uses to send it to the PBX. Every site that has its own PBX can define a PIN and a PIN template. Sites that share a PBX use the PIN and PIN template defined for the Global facility.

     For more information on Telephony-PINs, see Telephony PINs on page 196.

f. Expand the **Telephony - Dynamic Extensions** section and select the **Enable Dynamic Extensions** checkbox to assign dynamic extensions on demand to users who need them.

   - **Extension Range** — Enter a value for the **First Extension** and **Last Extension**
   - **Assignment Type** — Select one of the following two assignment types:
     - Choose **Permanent** to assign users extension that does not expire.
     - Choose **Temporary** to assign a lease duration value and specify the minimum amount of time that an extension is assigned to a user.

g. Expand the **Telephony - Sharing** section and click **Add** to specify information for other Facilities sharing this Telephony service information.

   You can add a **Facility** name, **Guest Access Number**, **Direct Access Number**, and the **Tie Line Prefix** information. For information on Telephony-Sharing configuration, see Shared Telephony Configuration.

6. Select one of the following to close the dialog.
   - **Save** — to add the new hospital location to the system.
   - **Cancel** — to return to the All Facilities page without adding a facility.

About Global Facility

Each Vocera Platform implementation has a facility named the Global facility.

Vocera creates the Global facility as a default. You cannot create or delete the Global facility manually; however, you can perform maintenance or modifications to the Global facility. For example, you can add and remove users from the Global facility, delete or add groups in the Global facility, and so forth.

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

- If your implementation doesn't involve multiple facilities, Vocera automatically associates all your entities with the Global facility.
- If your implementation doesn't involve multiple facilities, and you do not assign certain users, groups, locations, or contact entries to a specific facility (home location), Vocera automatically assigns them to the Global facility.

When you load data with a .CSV file that does not specify any information about the facility, Vocera automatically assigns all your entities to the Global facility.

Important: By default, every access point on your network is associated with the Global facility. If your deployment implements multiple facilities, you must assign a location name to each access point and associate each of these locations with a facility. Otherwise, the Voice Service always assumes that the Global facility is your current facility.

About Users and Telephone Numbers

If your facility 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:

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” contact.
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.

Access Code Exceptions

By default, Vocera uses the rules shown here to determine what access code to use with a telephone number.

- Any number within your local area code requires the Default Local Access Code.
- Any number that begins with a **0**, begins with an **X**, or has fewer than seven digits does not require an access code. Vocera treats numbers with fewer than seven digits as extensions.
- Any other number requires the Default Long-Distance Access Code.

If your organization uses any phone numbers that violate these rules, you must add entries that provide the access codes they require in the exception list. For example, you need to create an exception if an area code in addition to your local area code requires the Default Local Access Code instead of the Default Long-Distance Access Code.

Adding Access Code Exceptions

Use the **Telephony-Access Code Exceptions** section to add an entry to the list of exceptions on the Access Codes.

You can add exceptions to the entire area code, for a specific prefix, and a range of numbers in an area code.

Creating an Exception for a specific Area Code

To create an exception for the entire area code:

1. Navigate to the **Telephony-Access Code Exceptions** section in the Add/Edit Facility page.
2. Click **Add Exceptions** button to display the Add Access Code Exception dialog box.
3. Enter an area code number in the **Area Code** field.
   For example, enter 650 as the area code number.
4. Select **All numbers in area code** checkbox.
5. Enter an access code number in the **Access Code** field.
   For example, enter 9 as the access code number.
6. Click **Done** to save your entry and close the dialog box.
   The 650 area code appears as an exception on the Access Codes page.

Creating an Exception for a Specific Prefix

To create an exception for a specific prefix:

1. Navigate to the **Telephony-Access Code Exceptions** section in the Add/Edit Facility page.
2. Click **Add Exceptions** button to display the Add Access Code Exception dialog box.
3. Enter the area code the exception applies to in the **Area Code** field.
4. Check **Numbers starting with** and enter the prefix in the associated field.
5. Specify the access code in the **Access Code** field.
6. Click **Done** to save your entry and close the dialog box.

Creating an Exception for a Specific Range

To create an exception for a specific range:

1. Navigate to the **Telephony-Access Code Exceptions** section in the Add/Edit Facility page.

2. Click **Add Exceptions** button to display the Add Access Code Exception dialog box.
3. Enter the area code the exception applies to in the **Area Code** field.
4. Check **Numbers in range** and enter the beginning and ending numbers in the associated fields.
5. Use a seven-digit range in each field. To create an exception for a single number, enter the same number in both fields.
6. Specify the access code in the **Access Code** field.
7. Click **Done** to save your entry and close the dialog box.

Toll Exceptions

Use the Add Toll Exception dialog box to add an entry to the list of exceptions on the Toll Info page.

You must add an exception to this list in either of the following situations:

- When a number or range of numbers in your local area code is a toll call.
- When a number or range of numbers outside your area code is a toll-free call.

Adding Toll Exceptions

Use the **Telephony-Toll Exceptions** section to add an entry to the list of exceptions.You can create toll exceptions for an entire area code, for a specific exchange, and for a range of numbers in an area code.

To create an exception for an entire area code:

1. Navigate to the **Telephony-Toll Exceptions** section in the Add/Edit Facility page.
2. Click **Add Exception** button to display the Add Toll Exception dialog box.
3. Enter the area code the exception applies to in the **Area Code** field.
   Enter toll-free prefixes such as 800 and 888, as well as any area codes (such as 04 in Australia) that are toll-free in your dialing area.
4. In the **Match** section, choose one of the following options to define the range of DID numbers:
   - Choose **All Numbers in Area Code** to use the entire range of numbers represented by the value in the **Area Code** field.
     For example, If you add an 800 number in the **Area Code** field, an 800 prefix appears as a toll-free prefix in the list on the Toll Info page.
   - Choose **Numbers Starting With** and enter the exchange in the associated field.
     For example, if you want to specify that calls to the 427 exchange in your local 408 area code are toll calls, you can enter 408 in the **Area Code** field, select.**Numbers starting with** field and enter 427 in the associated field. Uncheck the **Toll-Free** field and click **Done**. The 427 exchange will appear as a toll exchange in the list on the Toll Info page.
   - Choose **Numbers in Range**
5. Select the **Toll-Free** field to specify a toll-free area code.
   Clear the **Toll-Free** field if you want the area code with toll.
6. Click **Done** to add your entry to the list and close the dialog box.

Direct Inward Dialing

In traditional telecommunications, Direct Inward Dialing (DID, or DDI in Europe) is the ability of a person outside an organization to call an internal PBX extension without going through an operator or intermediate interface of any kind.

When an outside caller dials a number within a specified DID range, the call goes directly to the associated user. Otherwise, the Genie prompts the caller to say the full name of the person or group, or enter an extension.

Vocera supports DID if you are using Vocera SIP Telephony Gateway and SIP signaling protocol. The DID feature allows callers who are not aware of Vocera or its features to contact users directly on their badges. DID extends the benefits of Vocera to telephone callers who do not necessarily even belong to the organization that is deploying Vocera.

To enable DID, your PBX administrator must reserve a range of DID numbers for Vocera to use, and you must identify that range to Vocera. Use the **Telephony-DID Information** section in the Add/Edit Facility page of the Web Console to specify the range of DID numbers reserved for Vocera.

Tip: The DID numbers that you specify must be 10-digit telephone numbers with area code in the US locale (or full numbers with city and region codes, in other locales).

If your PBX administrator provides a hunt group number as part of the DID range, enter it as the hunt number in Vocera, but do not include it in the range of DID numbers that you configure on the DID information page. User and group profiles may be assigned the DID numbers that you specify in the Web Console, and you do not want a user or group to have the same extension as the hunt number.

If an incoming call arrives on a number that is within the specified DID range, but the number is not assigned, Vocera automatically directs the call to the hunt group Genie.

When multiple facilities are sharing a PBX, they also share the single pool of DID numbers that are enabled in the primary facility. You cannot distribute different ranges of DID numbers to individual facilities that share a PBX.

When multiple facilities are using different PBXs, each PBX may provide a different range of DID numbers, or even none at all. The way each PBX is configured determines whether its associated facilities have access to DID.

Note: DID numbers may be more expensive and more difficult to obtain than other PBX extensions. You do not need to have a dedicated DID number for every badge to receive some of their benefits.

Adding or Editing DID Information

When you add or edit DID information, you specify a prefix and the range of phone numbers to use for direct inward dialing.

Your PBX administrator may provide you with discontinuous ranges of DID extensions or even groups of DID extensions with different prefixes. Enter each range separately until they all appear in the list on the DID Info page of the Telephony screen.

For example, your PBX administrator may supply 100 DID extensions with the following ranges:

- (215) 995-4150 through (215) 995-4199
- (215) 885-6880 through (215) 885-6899
- (215) 885-6920 through (215) 885-6949

You can enter each range separately in the Add DID Range Entry dialog box to make them all available to Vocera.

To add or edit DID information in the Add DID Range dialog box:

1. Navigate to the **Telephony-DID Information** section in the Add/Edit Facility page.
2. Click **Add DID** to display the Add DID Range dialog box.
3. Enter the area code and prefix assigned to the range in the **Prefix** field.

   For example, if the local area code of the PBX is 408, and the corporate prefix for all extensions is 790, you typically enter `(408)-790`. In some situations, your PBX administrator may assign a different prefix for you to use.

To provide maximum flexibility, Vocera does not check the value you enter in this field. If necessary, you may enter country and city codes, as well as extensions whose length is shorter or longer than four digits. For example, if your deployment has five-digit extensions, you may want to enter a prefix such as `(408)-79`.

Important: Enter the area code and full prefix that make a complete dialing string when combined with a value in the range of extensions. Vocera combines the extension and the value in the **Prefix** field to create a call-back number for paging.

4. In the **Match** section, choose one of the following options to define the range of DID numbers:
   - Choose **All Desk Extensions with Prefix** to use the entire range of numbers represented by the value in the **Prefix** field.
     For example:
     - If the value in the **Prefix** field is `(408)-790`, you are assigning the range `(408)-790-0000` through `(408)-790-9999` as DID extensions. The extensions available for assignment to Vocera users and groups are 000 through 999, 0000 through 9999, or 00000 through 99999.
     - If the value in the **Prefix** field is `5`, you are assigning any number that starts with a "5". The extensions available for assignment to Vocera users and groups are 500 through 599, 5000 through 5999, or 50000 through 59999.
   - Choose **Desk Extensions Starting With** and specify a starting value to use a subset of the range of numbers represented by the value in the **Prefix** field.
     For example:
     - If the value in the **Prefix** field is `(408)-790`, and you enter `8` in the **Desk Extensions Starting With** field, you are assigning the range `(408)-790-8000` through `(408)-790-8999` as DID extensions. The extensions available for assignment to Vocera users and groups are 8000 through 8999.
     - If the value in the **Prefix** field is `(408)-790`, and you enter **94** in the **Desk Extensions Starting With** field, you are assigning the range `(408)-790-9400` through `(408)-790-9499` as DID extensions. The extensions available for assignment to Vocera users and groups are 9400 through 9499.
     - If your PBX passes 59xx to Vocera, enter `5` in the **Prefix** field and `9` in the **Desk Extensions Starting With** field. This means you are assigning the range `5900` through `5999` as DID extensions. The extensions available for assignment to Vocera users and groups are 900 through 999.
   - Choose **Desk Extensions in Range** and enter beginning and ending values value to specify a range of phone numbers within the set represented by the value in the **Prefix** field. This is the most typical situation.
     For example:
     - If the value in the **Prefix** field is `(408)-790`, and you enter `8000 To 8999` in the **Desk Extensions In Range** field, you are assigning the range `(408)-790-8000` through `(408)-790-8999` as DID extensions. The extensions available for assignment to Vocera users and groups are 8000 through 8999.
     - If the value in the **Prefix** field is `5`, and you enter `501 To 549` in the **Desk Extensions In Range** field, you are assigning the range `5501` through `5549` as DID extensions. The extensions available for assignment to Vocera users and groups are 501 through 549.
5. Click **Done** to add your entry to the list and close the dialog box.

Telephony PINs

Telephony Personal Identification Numbers (PINs) allow your organization to authorize telephone usage, and to distribute telephone costs among different users, departments, or facilities.

Telephony PINs are also referred as Forced Authorization Codes (FAC) or Forced Access Codes in some organizations.

For example, a company might require employees to enter a PIN along with a phone number to make a long distance or toll call. Vocera's telephony PIN feature automatically adds a PIN to the dialing sequence when a user places a call that requires this PIN. In addition to long distance and toll calls, a PIN is also used for long distance forwarding, transferring, and paging.

Note: A user cannot make toll calls—and telephony PINs have no effect if the user is not a member of a group that allows toll calls.

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 3: 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 4: PIN template examples

PIN template	Result	Description
%N %P	912135550945 1234	Access code, phone number, PIN.
%M %P	2135550945 1234	Phone number, PIN.

PIN template	Result	Description
%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

Specifying Telephony PIN Information For a Site

1. Click **Telephony** in the navigation bar.
2. Click the Basic Info tab to display the **Basic Info** page. In this page, the **Enable Telephony Integration** check box must be checked before you can enter information in the PIN page.
3. Click the **PIN** tab to display a page where you can enter a site-level PIN and define a template that specifies how to integrate a PIN into a dialing sequence.
4. Use the **Select Site** field to choose the site you want to configure.

   Every site that has its own telephony server can specify a PIN and a PIN template. Sites that share a telephony server use the PIN and PIN template defined for the **Global** site. To configure a single-site environment, choose the **Global** site.
5. (Optional) Type a number in the **PIN for Long Distance Calls** field to define a site-level PIN.
6. Type numbers, formatting characters (for example, dashes or parentheses) special dialing characters (for example, commas or ampersands), and PIN macros in the **PIN Template** field. This template defines the format of all PINs, whether they are defined at the user, department group, or site level.

   If no PIN template is specified, the Vocera system applies one of the following default templates, depending on the type of PBX:

   Table 5: Default PIN templates

PBX type	Default template	Description
IP	%N %P	Access code, phone number, and PIN.

Dynamic Extensions

To allow Vocera users to receive paging call-backs on their Vocera device, each user must have a unique extension entered in their Vocera profile.

You must enter a value in either the **Vocera Extension** field or the **Desk Phone or Extension** field for each user. You can assign these values manually, or you can let Vocera assign them as dynamic extensions.

Configuring Dynamic Extension for a Facility

Configure Vocera system to supply telephone extensions on demand to users who need them.

Dynamic extensions affect only users whose profile does not include a Vocera extension or a desk extension. For additional information on phone fields and users see About Users and Telephone Numbers on page 192.

Vocera assigns dynamic extensions to users in a manner analogous to a DHCP server assigning IP addresses to client computers.

1. Navigate to **Facilities** in the **Manage** section of the navigation bar and locate your facility.

   If you don't have a facility set up, follow the instructions described in the, "Adding a Facility" section of the Vocera Platform Administration Guide to create a new facility.

Tip: You can also use the **Help** link provided in the **Facilities** page of the Vocera Platform Web Console and follow the instruction to create a new facility.

2. Scroll down to the **Telephony - Dynamic Extensions** section ane expand this section to view the **Enable Dynamic Extensions** checkbox.
3. Select the **Enable Dynamic Extensions** checkbox to assign dynamic extensions on demand to users who need them.
   The **Extension Range** and **Assignment Type** configuraiton fields are displayed.
4. Enter a value for the following fields:
   - **Extension Range** — Specify a range of phone numbers to use as dynamic extensions. Enter a value for the **First Extension** and **Last Extension**.

     Note: If the range is equal to or a subset of the range you entered for DID, Vocera assumes you are distributing DID extensions among your Vocera users. If you are using DID, set the dynamic extension range to be the same as the DID range. If the dynamic extension range is a subset of the DID range, some DIDs will not be used. If the range is not a subset of the range you entered for DID, Vocera assumes that you want to assign desk extensions to users independently of DID.
   - **Assignment Type** — Select one of the following two assignment types:
     - Choose **Permanent** to assign users extension that does not expire.
       Permanent is useful when Vocera users do not have actual desk extensions, but you want them to have a unique identifier that allows recipients of a numeric page to place a return call to the Vocera device.
     - Choose **Temporary** to assign a lease duration value and specify the minimum amount of time that an extension is assigned to a user.
       Temporary is useful when you want to share a small number of DID extensions among a larger number of Vocera users. By default, the lease is set to seven days to allow safe paging callbacks several days later. If you don't have enough DID numbers for all Vocera users, you can set the lease duration to hours instead of days so that numbers can be reallocated as needed.
5. Select one of the following to close the Add/Edit Facilities page:
   - **Save** — to save the telephony dynamic extensions information to the system.
   - **Cancel** — to cancel the changes and return back to Add/Edit Facilities page.

Shared Telephony Configuration

When you configure two or more facilities to share a telephony service, enable telephony for one facility only. The facility for which telephony is enabled is considered the principal facility. Facilities that use the shared telephony service of a principal facility are called secondary facilities.

Do not enable telephony for secondary facilities that use the telephony service of a principal facility. Instead, use the **Telephony- Sharing** section to configure the principal facility to share the telephony service with the other facilities.

On the principal facility's **Telephony-Sharing** section, click **Add** to display the Add Shared Telephony Info dialog box. Specify the name of the facility that is sharing the principal's telephony service, then do one of the following:

- **If the facilities have the same hunt group numbers:**
  Leave the **Guest Access Number**, **Direct Access Number**, and **Tie Line Prefix** fields blank.
  This configuration specifies that Vocera will search the combined grammars of the principal and sharing facility when incoming callers respond to the hunt group Genie.
- **If the facilities have different hunt group numbers:**

If using Vocera SIP Telephony Gateway for telephony integration, enter values in the **Guest Access Number** and **Direct Access Number** fields. Leave the **Tie Line Prefix** fields blank.
This configuration specifies that Vocera will search only the grammars for a facility as specified by the hunt group numbers or line numbers when incoming callers respond to the hunt group Genie.

Adding and Editing Telephony Sharing Information

When you add or edit telephony sharing information, you specify the names of the secondary facilities that are using the principal facility's shared telephony service. You also optionally specify the hunt group numbers and trunk lines used by the secondary facilities.

Note: You must enable telephony for the principal facility before you share it. Use the Telephony - Basic Information of the Add New Facility screen to enable the telephony integration, as described in Adding a Facility.

To add or edit telephony sharing information from the Add Shared Telephony Info dialog box:

1. Enter or edit the following information:

   Table 6: Shared telephony information fields

Field	Description
Facility	Specify a secondary facility that will use the shared telephony service of the principal facility. **Important:** The site you select cannot be a principal facility with telephony enabled. If you select a principal facility with telephony enabled, the system automatically disables telephony for that facility.
Guest Access Number	Optionally specify the area code and phone number of a DID line or hunt group for this site. This number is for guest access to the Vocera system. When callers dial the **Guest Access Number**, they are allowed to place a call but are not identified to the called person. Because guest users are not authenticated, they can call other users but they cannot issue voice commands. • If you want the secondary facility to have the same Guest Access number as the primary facility, leave this field blank or enter the primary facility's Guest Access number. • If you want the secondary facility to have a different Guest Access number, coordinate with your PBX administrator, then enter the number.
Direct Access Number	Optionally specify the area code and phone number of a DID line for this facility. 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 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.
Tie Line Prefix	Specify the prefix of the dial string used to place calls through the tie line to the selected facility that is sharing the principal's telephony service. Alternatively, this field could also be used to specify a prefix for Direct Inward Dialing (DID) numbers at the selected facility. For tie lines, enter the tie prefix plus the tie line. For example, if the tie prefix is 8 and the tie line is 257, enter `8-257`. For DID numbers, identify the DID prefix by determining the constant digits that become the prefix to an extension to produce a full DID number. For example, if the format of your DID numbers is 408-882-nnnn, the DID prefix is `408-882`. In the US locale, the full DID number must be a 10-digit telephone number that includes the area code. In other locales, full DID numbers include city and region codes. The Vocera Platform prepends the Tie Line Prefix to the extension dialed to generate the complete dial string for the selected facility. If the selected facility does not have its own PBX and a tie line or DID numbers, leave this field blank. **Note:** The Tie Line Prefix is used for all extensions dialed for the selected facility. Only one Tie Line Prefix can be used per shared facility.

2. Click **Done** to add this facility to the list and close the dialog box.

Initiating Emergency Broadcasts Silently

You can set up your facility to initiate an emergency broadcast silently, without playing a chime.

Emergency broadcasts are initiated on the Vocera device when you click the Call button on your Vocera device twice. You can also initiate an emergency broadcast from the Vocera Collaboration Suite on your cell phone, see About Emergency Broadcast for more information.

Before you initiate a silent emergency broadcast you must set up the emergency broadcast group.

1. Click **Add New Facility** or select **Edit Facility** from the **Options** button for the Facility settings that you want to modify.
   The New Facility/Edit Facility page appears.
2. In the General section, click **Find Group** button to select a group as the Emergency Broadcast group.
   Skip this step if there is an Emergency Group already selected for this facility.
3. Select the **Initiate Emergency Broadcast Silently** checkbox.
4. Choose one of the following to close the dialog:
   - **Save** — to update the facility configuration changes.
   - **Cancel** — to return to the Facilities page.

Playing with Easter Eggs

Easter Eggs are a set of voice commands that you can use to get some funny responses to your questions from Vocera Genie

Easter eggs are secret messages or jokes intentionally hidden within the Vocera software. Badge user can use the Easter Eggs voice commands to reduce tension, distract or calm children, or simply have fun.

The name, “Easter Eggs” is borrowed from the Easter holiday ritual of hunting for Easter eggs, where children hunt for eggs that often contain surprises and treasures.

The Easter Eggs feature is enabled at the Facility level in the by default. You can disable Easter Eggs for badge users in a Facility, see the Disabling Easter Eggs section for more information.

To access an Easter Eggs commands, press the Call button on the badge and say one of the Easter Egg commands listed in the Vocera Voice Commands Reference Guide. For guidelines on using the commands, see your supported Vocera Device User Guide on the Vocera Devices page.

Disabling Easter Eggs

You can disable Easter Eggs feature for users in a Facility.

Easter Eggs are enabled by default at the Facility level. You can disable Easter Eggs from the Web Console if you find this feature inappropriate or unnecessary for badge users associated with a specific Facility.

To disable the Easter Eggs feature:

1. Click **Facilities** in the navigation bar.
   The All Facilities page displays with a list of hospital locations in your system.
2. Choose a Facility name from the list or type a name in the search bar.
   The Search bar helps you to find a facility name quickly. As you start typing a name, Search retrieves the closest match in your lists of facilities.
3. Click **Edit Facility** from the dropdown menu in the **Options** button.
   The Edit Facility page appears with fields that you can modify.
4. In the General section, uncheck the **Enable Easter Eggs** checkbox to disable the Easter Eggs feature.
5. Click **Save**.

After your disable this feature, when a user says an Easter Eggs voice command, for example, “Santa Claus”, Genie responds with the following:

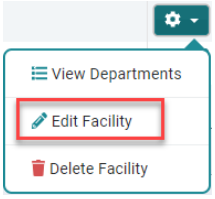
“Sorry, you do not have permissions to play Easter Eggs, please see your administrator.”

Editing a Facility

You can edit the information for any existing hospital location from the Vocera Platform Web Console.

1. Select **Facilities** in the **Manage** section.
   The Hospital Locations page displays. The All Facilities section displays the facility name (in alphabetical order), number of departments in a facility, and a description of each facility.
2. Locate the hospital location that you want to edit in the alphabetical list.
3. Click the **Options** button in the far right of this facility.

4. Select **Edit Facility** from the dropdown menu.



   The Edit Facility page appears with configuration fields and data related to the configuration fields.
5. Complete the fields listed in the table below. An asterisk * indicates that a value must be entered for this field.

Name	Maximum Length	Description
Name *	100	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.
Description	100	An optional abbreviation to represent this facility name.
Time Zone*	n/a	Use the **Time Zone** dropdown menu to select a time zone for the facility.
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 facility. You also set an emergency group for each functional group in your organization. For more information, see About Emergency Broadcast.
Enable Code Lavender	n/a	Check the **Enable Code Lavender** checkbox to enable Code Lavender for this facility. This option is off (unchecked) by default. For more information on configuring Code Lavender, see Configuring Code Lavender on page 180.
Enable Easter Eggs	n/a	Uncheck the **Enable Easter Eggs** checkbox to disable the Easter Eggs commands. This option is enabled (checked) by default. For more information on Easter Eggs, see Playing with Easter Eggs on page 201.

Name	Maximum Length	Description
Initiate Emergency Broadcast Silently	n/a	Specifies whether to initiate emergency broadcasts at this facility silently, that is, without playing a chime first. This option is available only if a group is specified in the **Emergency Broadcast Group** field at the facility and group. By default, the option is not selected, see Initiating Emergency Broadcast Silently for more information. **Note:** This field is not available for **Groups**. A silent emergency broadcast is configured at the **Facilities** level only and applies to all emergency groups for the entire facility including panic groups set per group.

If Voice Service is used, provide the following information.

Name	Maximum Length	Description
Cost Center	100	(Optional) Use the **Cost Center** field to specify a cost center for the facility.
Alternate Spoken Name	50	(Optional) Use the **Alternate Spoken Name** field to enable Vocera to recognize variations of the exact facility name. For example, if users commonly refer to a facility by a nickname or an acronym, enter that variation here.
Spoken Name Count	n/a	(Optional) The **Spoken Name Count** field displays the total number of names that you can use in a voice command for this facility. It includes the names of users, groups, facilities, contacts 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.

6. Select the **Enable Telephony Integration** checkbox to allow Vocera and your phone system to communicate with each other and configure the fields related to basic telephony information.

   When the **Enable Telephony Integration** checkbox is not selected, all telephony related fields are also disabled.

   You can clear the **Enable Telephony Integration** checkbox and click the **Save** button to disable telephony features for a facility. Vocera saves your telephony settings but disables communication to the PBX.

   a. Enter the **Telephony - Basic Information** for the following fields:

Name	Maximum Length	Description
Number of Lines	3 digits	Specify the number of lines you want to provision for each telephony service in the **Number of Lines** field. Enter either of the following values, whichever is smaller: • The number of lines supported by your license. • The number of lines provisioned by the PBX for a single telephony service. If you are configuring a high availability array, enter the number of lines available to a single telephony service, not the total number of lines available to all services. For example, if you have 2 Vocera SIP Telephony Gateway (VSTG) services and your license contains 48 lines, specify 24 in this field to give each service 24 lines for a total of 48. The number of lines that you provision for each telephony service is decremented from the number of lines in your license.
Local Area Code	3 digits	Enter the area code of the region in which the Voice Service is installed in the Local Area Code field.
Omit Area Code when Dialing Locally	n/a	Check the Omit Area Code field when dialing locally. If your PBX requires you to dial local calls without using the area code you can enable this option. By default, Vocera includes the area code in the dialing string, even when dialing a local number. Check this field if your PBX or locale requires you to omit the area code when dialing local calls.
Voice Hunt Group	n/a	Specify the area code and phone numbers of the DID lines or hunt group you set up for the Vocera system in the **Vocera Hunt Group Numbers** fields. There are two hunt group number fields: • **Guest Access** — This number is for guest access to the Vocera system. When callers dial the Guest Access number, they are allowed to place a call but are not identified to the called person. Because guest users are not authenticated, they can call other users, but they cannot issue voice commands. To use the **Guest Access** number with numeric pagers, enter an asterisk after the last digit of the phone number. When a user sends a numeric page, Vocera passes the value that you enter in this field to the pager and then passes the user's desk extension to the pager. Some pagers display the asterisk as a hyphen, separating the desk extension from the Vocera number. • **Direct Access** — This number is for specially licensed user access to the Vocera system. This field is used only if 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** phone number from their desk phone or cell phone.
Default Local Access Code	n/a	Specify the sequence of numbers you use to get an outside line. For example, a PBX might require you to dial a 0 or a 9 or an 8 to get an outside line. By default, Vocera prepends this access code to any number within the local area code.

Name	Maximum Length	Description
Default Long-Distance Access Code	n/a	Specify the sequence of numbers you enter before placing a long distance call. For example, a PBX system might require you to dial a 9 to get an outside line and then dial a 1 before a long-distance telephone number. In this situation, the Default Long-Distance Access Code is 91. By default, Vocera prepends this access code to any number that includes an area code that is not the local area code.
Company Voicemail Access Code	n/a	Use the Company Voicemail Access Code field to specify the sequence of numbers you use to access the company's voice mail system. A typical entry includes X, then the sequence of digits that you dial to get into the voicemail system from an internal phone, and possibly special dialing characters such as the * or # to indicate the end of the sequence.
SIP Settings	n/a	Specify the SIP settings: • **Call Signaling Address** — Enter the call signaling address for your IP PBX or VoIP gateway. For PBX failover support, enter a comma-separated list (up to 256 characters) of call signaling addresses for two or more PBXs or gateways in order of preference. Enter each call signaling address in this format: `IP_Address:Port` The `Port` is optional. If you do not specify a port, port 5060 (the default) is used. VSTG uses only one PBX or gateway at a time. If you specify multiple call signaling addresses, VSTG tries each PBX or gateway in the order specified and uses the first one that responds. If that PBX or gateway goes down, Vocera SIP Telephony Gateway switches to another one. The preference order of call signaling addresses is important. If the Vocera SIP Telephony Gateway is currently using the PBX for the second call signaling address, and then the PBX for the first call signaling address becomes active, Vocera SIP Telephony Gateway automatically switches to the first PBX. **Note:** The Vocera SIP Telephony Gateway uses the response to a SIP OPTIONS message to determine if the PBX or gateway is currently available. The OPTIONS message is sent every 30 seconds by default. For more information on configuring Vocera SIP Telephony Gateway to use an OPTIONS message for keep-alive, see Detecting the Connection to the IP PBX. If the PBX or gateway is not configured to support SIP OPTIONS, then entering a second call signaling address has no effect. In some situations, using TCP as the signaling transport protocol reduces the length of time required for the VSTG to recognize that the current PBX is down and move to the next PBX in the list. • **Call Party Number** — Enter the DID number, including the area code, of the Vocera trunk (the number of digits depends on the locale). Outgoing calls use this value as the caller ID. However, you can configure Vocera SIP Telephony Gateway to use caller information contained in the dial signal from the Voice Service as the caller ID.

b. Expand the **Telephony - Access Code Exceptions** section and click **Add Exceptions** to add an exception for the entire area code, a specific prefix, or for a range of numbers within an area code.

By default, numbers in the local area code use the Default Local Access Code, and all others use the Default Long-Distance Access Code. For more information on Telephony-Access Code Exceptions, see Access Code Exceptions more information.

c. Expand the **Telephony - Toll Exceptions** section and click **Add Exceptions** to add any exceptions for an entire area code, a specific prefix, or for a range of numbers within an area code.

   You must add an exception to this list in either of the following situations:

   - When a number or range of numbers in your local area code is a toll call.
   - When a number or range of numbers outside your area code is a toll-free call.

   For more information on Toll Exception configuration, see Toll Exceptions.

d. Expand the **Telephony -DID Information** section and click **Add DID** to specify the range of Direct Inward Dialing (DID) extensions that are available for use by Vocera users.

   If your PBX administrator provides a hunt group number as part of the DID range, do not include it in the range of DID extensions you specify here. The extensions on this page are for use by users only.

   For more information on DID configuration, see Direct Inward Dialing.

e. Specify Telephony Personal Identification Numbers (PINs) in **Telephony -PINs** section.

   - **PIN for Long Distance Calls** — Enter a PIN for a facility. If a telephony PIN is not specified in the user's profile, and the user does not belong to a group that has a PIN, then the facility PIN is used. The facility-level telephony PIN is used for long distance numbers specified in Contacts. It is also used for group forwarding numbers, unless the group is a department group with a PIN number specified, in which case the department group PIN is used.
   - **PIN Template**— Specify a template for adding a PIN to a dialing sequence. A PIN template can include digits, special characters, and PIN macros.

     When a dialing sequence includes a PIN, this value defines the format that the Vocera system uses to send it to the PBX. Every site that has its own PBX can define a PIN and a PIN template. Sites that share a PBX use the PIN and PIN template defined for the Global facility.

     For more information on Telephony-PINs, see Telephony PINs on page 196.

f. Expand the **Telephony - Dynamic Extensions** section and select the **Enable Dynamic Extensions** checkbox to assign dynamic extensions on demand to users who need them.

   - **Extension Range** — Enter a value for the **First Extension** and **Last Extension**
   - **Assignment Type** — Select one of the following two assignment types:
     - Choose **Permanent** to assign users extension that does not expire.
     - Choose **Temporary** to assign a lease duration value and specify the minimum amount of time that an extension is assigned to a user.

g. Expand the **Telephony - Sharing** section and click **Add** to specify information for other Facilities sharing this Telephony service information.

   You can add a **Facility** name, **Guest Access Number**, **Direct Access Number**, and the **Tie Line Prefix** information. For information on Telephony-Sharing configuration, see Shared Telephony Configuration.

7. Select one of the following to close the dialog.
   - **Save** — to update the facility information in the system.
   - **Cancel** — to return to the Hospital Locations (All Facilities) page.

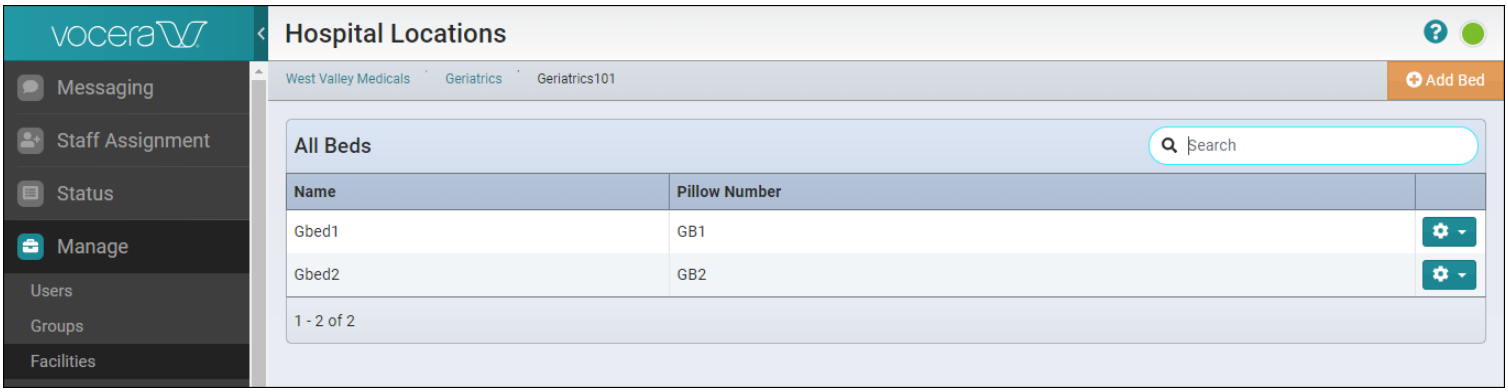
About Departments, Rooms, and Beds

Create an entry for the departments, rooms, and beds that are associated with each hospital location (facility).

You can view, add, edit, and remove components in a hospital location easily from the **Manage** section in the navigation bar of the Vocera Platform Web Console. Select a hospital location in **Facilities**, and then use the **Options** menu to drill down to departments, rooms, and finally beds.

Alternatively, you can also click on a facility to view the departments associated with this facility, click on a department to view rooms associated with this department, and click on a room to view the beds and pillows assigned for this room.

The following screenshot displays a Facility named West Valley Medicals with a Department named Geriatrics, and a room named Geriatrics 101 with beds (Gbed1 and Gbed2) and pillow number information.



When you delete a hospital location from the system, the associated departments, rooms, and beds are also removed from the system.

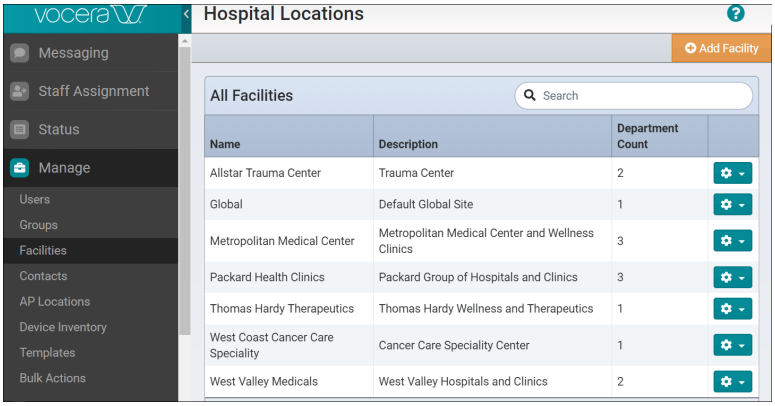
For example, when deleting a room from a department, any beds in the room are also removed from the system. A warning dialog alerts you of the components affected by the delete activity and provides the opportunity to proceed or to abort the deletion.

Working with Departments

You can view the departments created for any specific hospital locations.

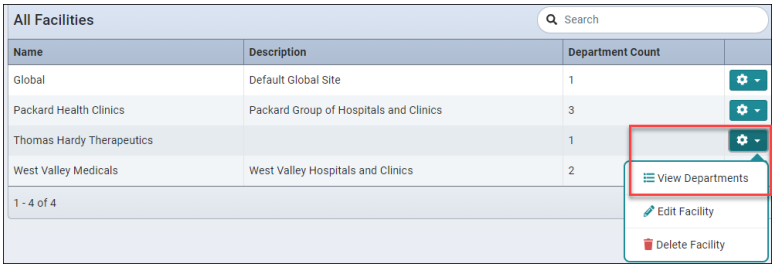
Access the Vocera Platform Web Console to view a department in a hospital location.

1. In the Hospital Locations page, locate the facility for which you want to view the departments.
   The All Facilities panel displays the facility names in alphabetical order, the number departments in each location, and an **Options** button to access a navigation menu.



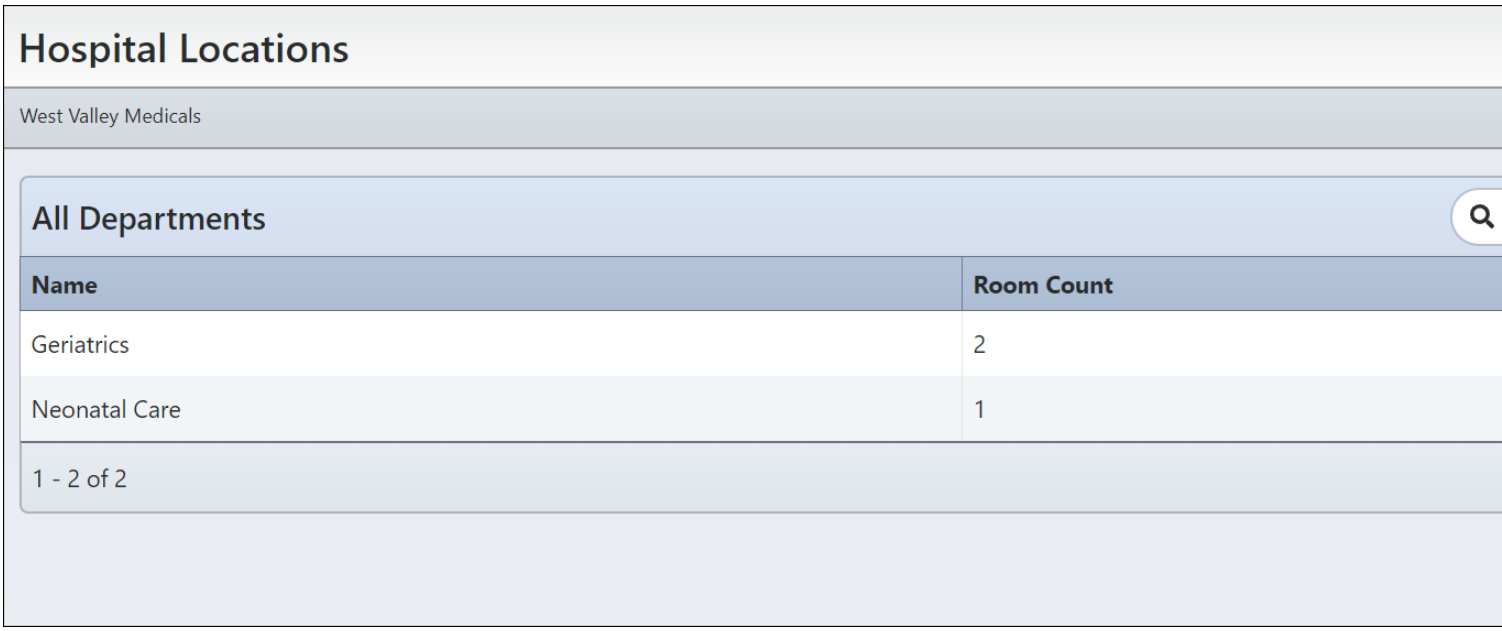
2. Click the **Options** button in the far right of this hospital location's row.

3. Select **View Departments** from the Options dropdown menu.



The All Departments page displays with a list of departments defined for this hospital location.

4. Select the dropdown menu to edit or delete the department. You can also select the **View Rooms** option to view all the rooms assigned for this department.



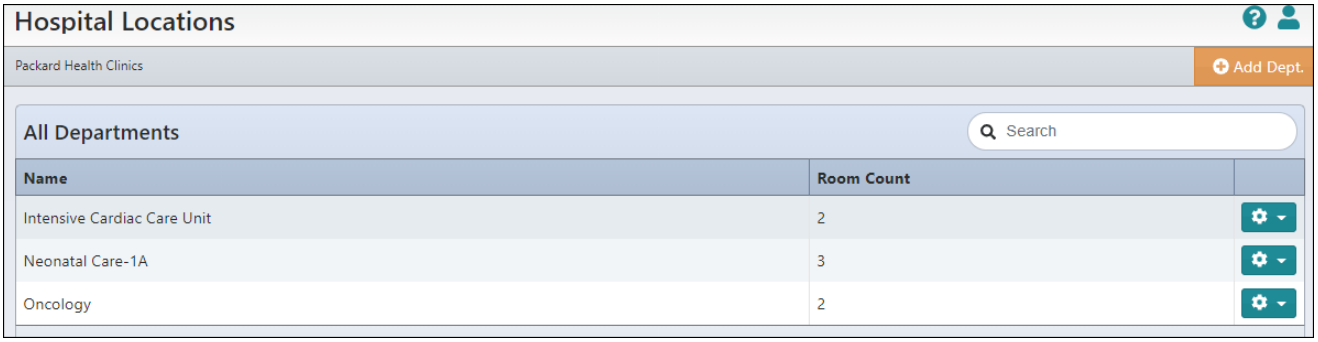
Adding a Department

For any hospital location, you can specify departments. Each department is a logical or physical organization within a facility, such as a floor or a wing.

Note: All departments are associated to a facility, you cannot create a department without creating a facility.

To add a department to a facility:

1. Navigate to **Facilities** in the **Manage** section of the navigation bar.
2. In the All Facilities page, identify the facility where you want to add a department.
   The All Departments page displays any existing department names in alphabetical order along with the number of rooms allocated to each department.



3. Click **Add Dept.** in far right corner

   The New Department page displays.
4. In the General section, specify a name for your new department in the **Name*** field in the General section.

   An asterisk * indicates that the field must be provided.
5. In the Assignment Permissions section, click **Add** to display the Find a Group dialog box.

   Use the Find a Group dialog to:
   - Enter the group name in the **Group Name** field to search for a group in system.
   - Select multiple groups from the list.
   - Toggle the **Facility Name** field to view all facilities available in your system and refine your search.
6. In the **Group Name** field, enter the name of the group that you want to allow to make assignments within the department.

   You can also select more than one group names from the Find a Group dialog box and click to allow multiple groups to make assignments within the department.
7. Click **Select Groups** to close the Find a Group dialog.
8. Select one of the following to close the dialog:
   - **Save** — to add the new department to the system.
   - **Cancel** — to return back to the All Department page without adding a department.

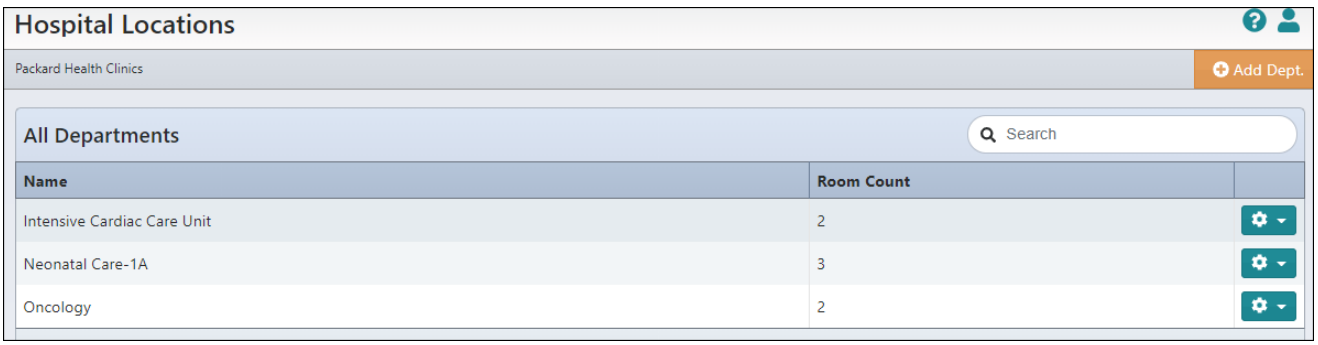
Editing a Department

After you have created a department for a hospital location, you can edit its information.

Access the Vocera Platform Web Console to edit a department belonging to a facility.

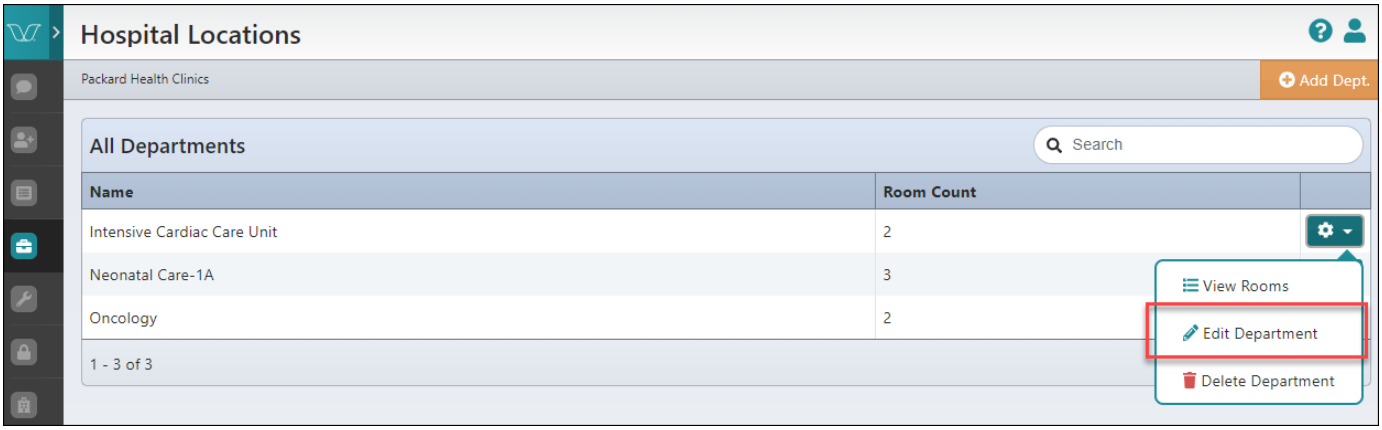
1. Navigate to **Facilities** in the **Manage** section of the navigation bar, and select a facility associated with the department that you want to edit.
2. Click on the selected Facility to display all departments in this facility.

   The All Departments page displays the department names in alphabetical order and the number of rooms in each department.



3. Click the **Options** button in the far right of the department's row that you wish to edit.

4. Select **Edit Department** in the drop down menu.



The Edit Department page displays.

5. In the Assignment Permissions section, click **Add** to display the Find a Group dialog box.

   Use the Find a Group dialog to:

   - Enter the group name in the **Group Name** field to search for a group in system.
   - Select multiple groups from the list.
   - Toggle the **Facility Name** field to view all facilities available in your system and refine your search.

6. In the **Group Name** field, enter the name of the group that you want to allow to make assignments within the department.

   You can also select more than one group names from the Find a Group dialog box and click to allow multiple groups to make assignments within the department.

7. Click **Select Groups** to close the Find a Group dialog.
8. Select one of the following to close the Edit Department page:

   - **Save**— to save the edited department in the system.
   - **Cancel**— to return back to the All departments page without changing the department name.

Deleting a Department

You can delete a department from a facility.

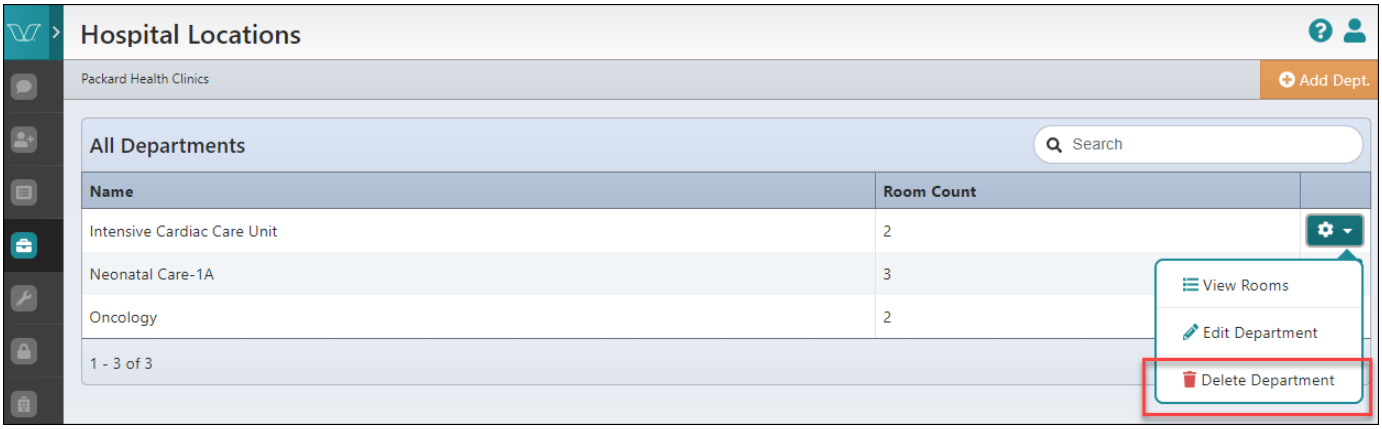
Access the Vocera Platform Web Console to delete a department from a facility.

1. Navigate to **Facilities >All Departments** and select a department that you want to delete.

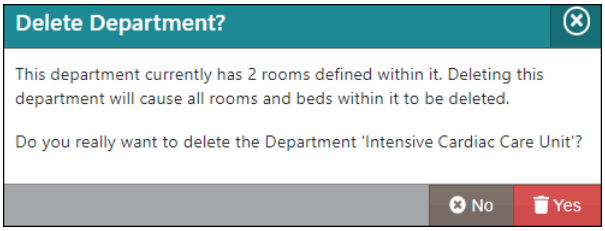
   The All Departments page displays the department names in alphabetical order along with the number of rooms in each department.

2. Click the **Options** button in the far right of the department's row that you wish to view.

3. Select **Delete Department** in the Options drop down menu.

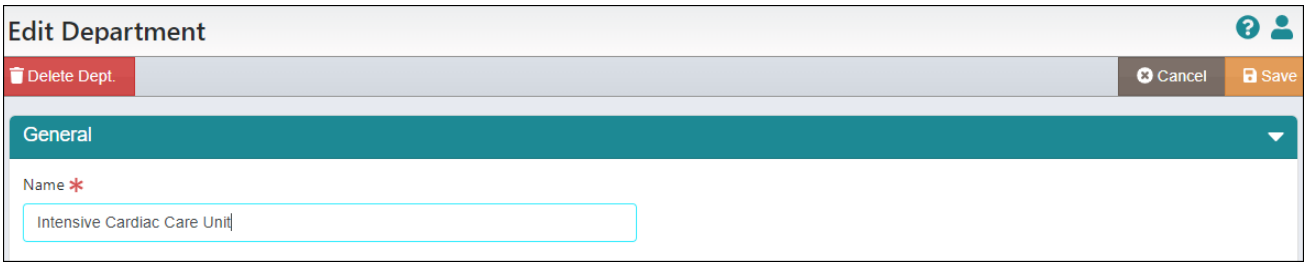


The Delete Department dialog box displays:



4. Select one of the following to close the Delete Department dialog.
   - **No** — to cancel the delete action and return to the All Department page without deleting a department.
   - **Yes** — to confirm the delete action.
     Delete department will delete all rooms and beds belonging to this department from the system.

You can also perform the delete action from the Actions bar while editing and making changes to the department.

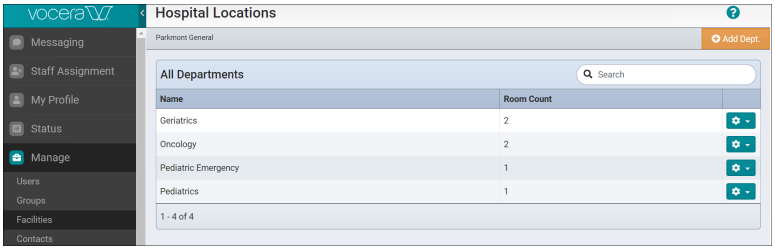


Click the **Delete Dept.** button to delete the department that you are editing. The system will display a confirmation dialog box as mentioned in Step 3.

Working with Rooms

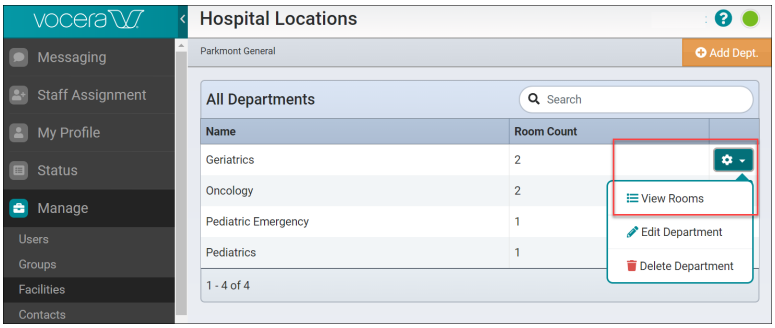
You can display the rooms defined in the system for any specific department of a hospital location.

1. Navigate to the facility and select the department where you wish to add rooms or remove existing rooms.
   The All Departments page displays the department names in alphabetical order, the number of rooms in each department, and an **Options** button to access a dropdown menu.



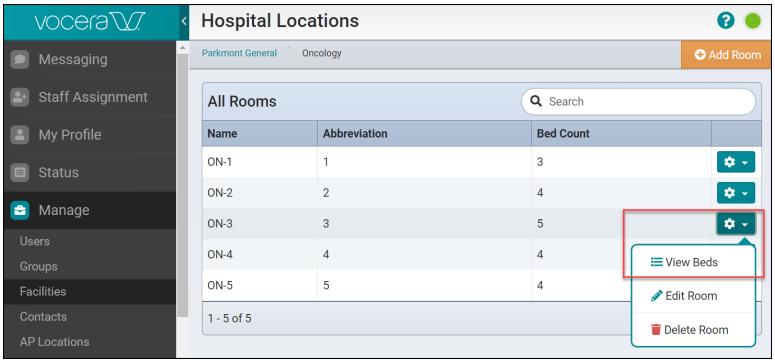
2. Click the **Options** button in the far right of this hospital department's row.

3. Select **View Rooms** from the Options popup menu that appears.



The All Rooms page displays the rooms allocated for this hospital department.

4. From the All Rooms page, you can add, edit, or delete rooms for the hospital and department shown in the Action menu.

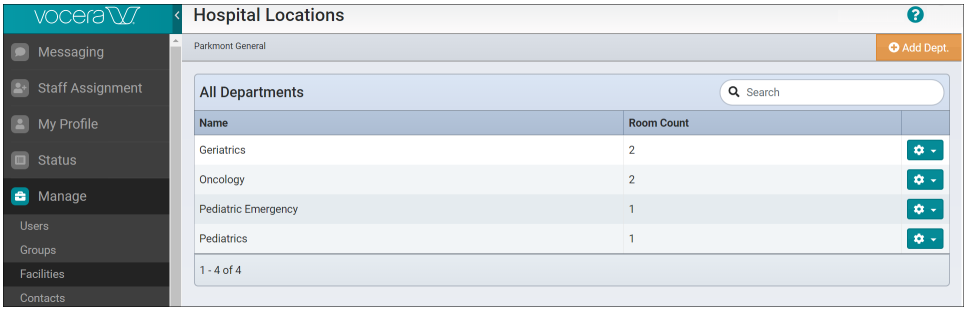


Adding a Room

For any department in a hospital location, you can add a room to the list of defined rooms.

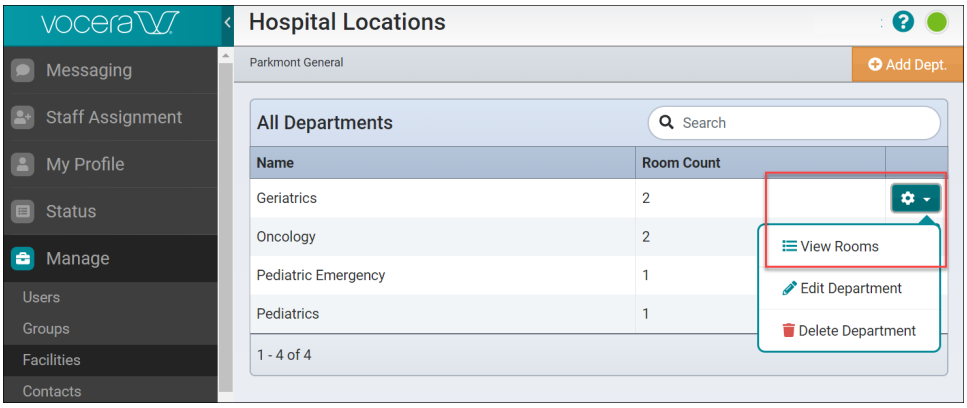
Access the Vocera Platform Web Console to add a room to a department in a Physical Location.

1. Navigate to the facility and departments where you wish to work with rooms.
   Verify the facility name in the breadcrumbs in the Actions bar.



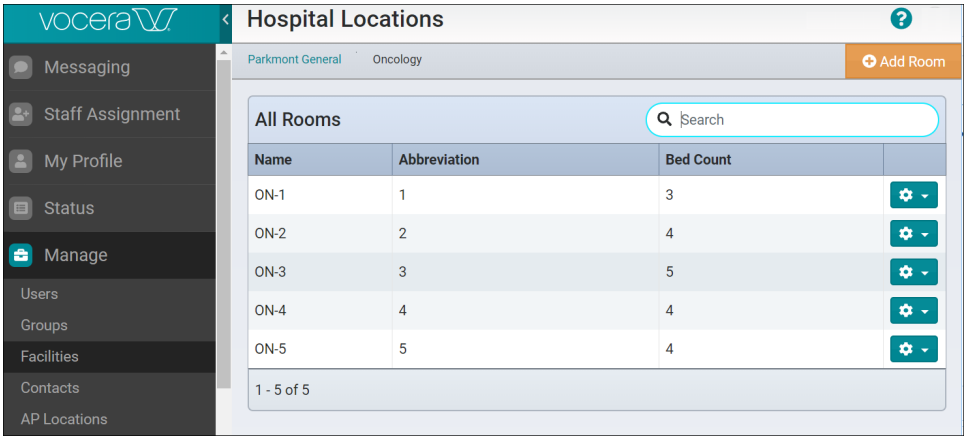
2. Click the **Options** button in the far right of the departments row.

3. Select **View Rooms** from the popup menu that appears.



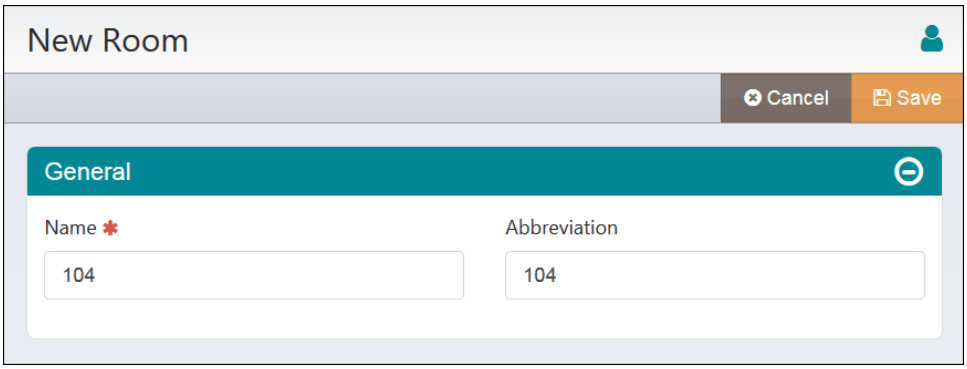
The All Rooms page displays all the rooms allocated to department.

4. Click **Add Room** in the Actions menu.



The New Room page displays.

5. In the General section, click the cursor in the **Name** field and start typing a name or number.



Name	Description
Name *	The name of the new room.
Abbreviation	An optional abbreviation to represent this room name.

An asterisk * indicates that the field must be provided.

6. Select one of the following to close the dialog.

- **Save** — to add a new room to the system.
- **Cancel** — to return back to the All Rooms page without adding a room.

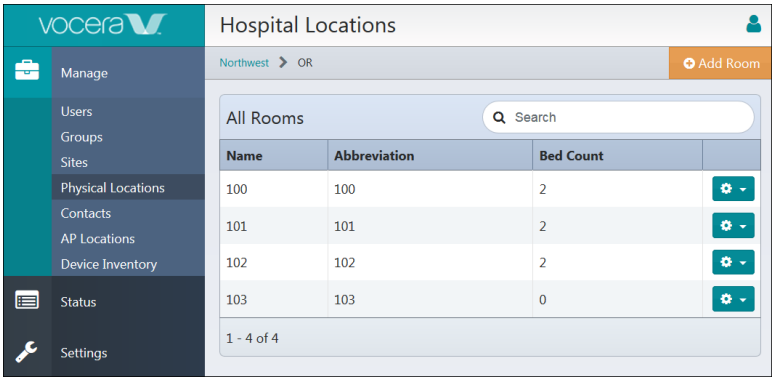
Editing a Room

After you create a room in a department, you can edit the information specific to this room.

Access the Vocera Platform Web Console to edit a room belonging to a room in a Physical Location.

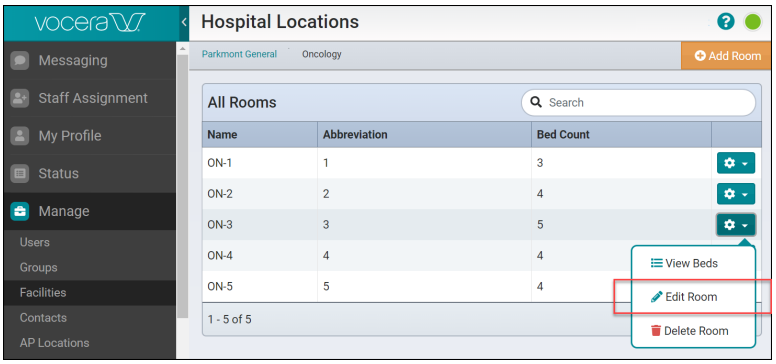
1. Navigate to All Rooms in the room where you wish to edit a room. See Working with Rooms on page 211.

   Verify the correct physical location in the Actions breadcrumbs. The All Rooms panel displays the room names in numerical order, a name abbreviation for each room, the number of beds in each room, and an Options button to access a navigation menu.

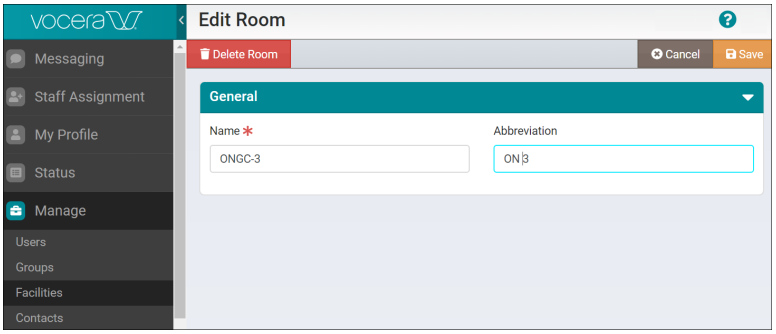


2. Click the **Options** button in the far right of this hospital room's row.

3. Select **Edit Room** in the **Options** dropdown menu.



   The Edit Room page displays.



4. In the General section, enter a value for the fields listed in the table below.

An asterisk * indicates that the field must be provided.

Name	Description
Name *	The name of the room.
Abbreviation	The abbreviated name of the room.

5. Select one of the following to close the dialog.
   - **Save** — to save changes in the system.
   - **Cancel** — to return back to the All Rooms page without changing a room.

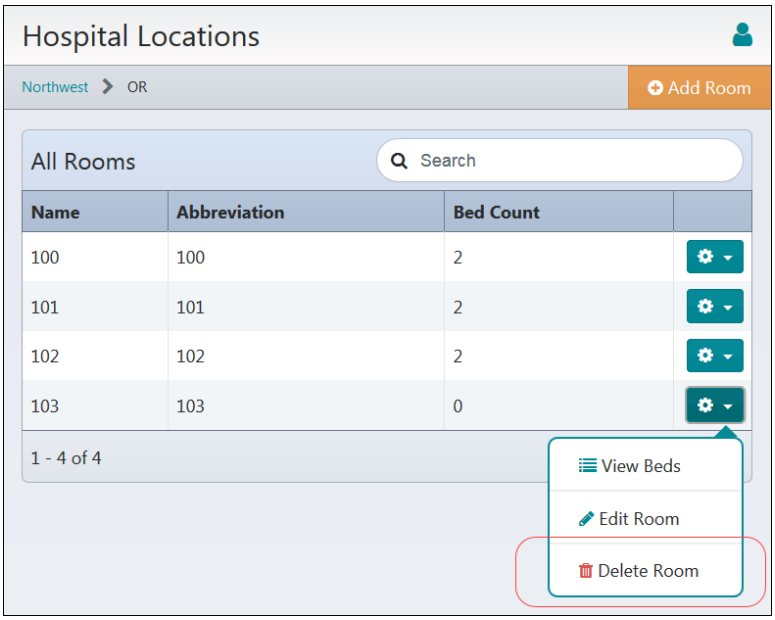
Deleting a Room

You can delete a room from a facility.

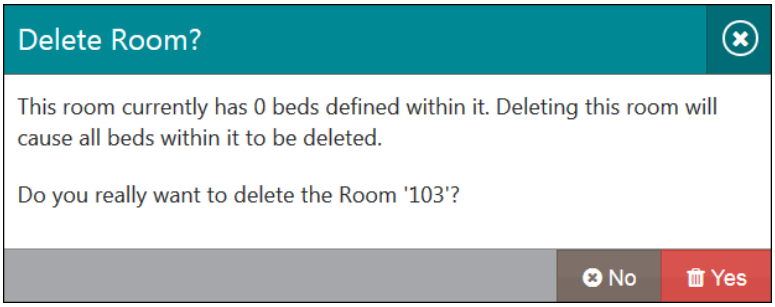
Access the Vocera Platform Web Console to delete a room from a facility in a Physical Location.

1. Navigate to the All Rooms window in the room where you wish to edit a room.
   The All Rooms panel displays the room names in numerical order, a name abbreviation for each room, the number of beds in each room, and an Options button to access a navigation menu.
2. Click the **Options** button in the far right of the room's row that you wish to view.

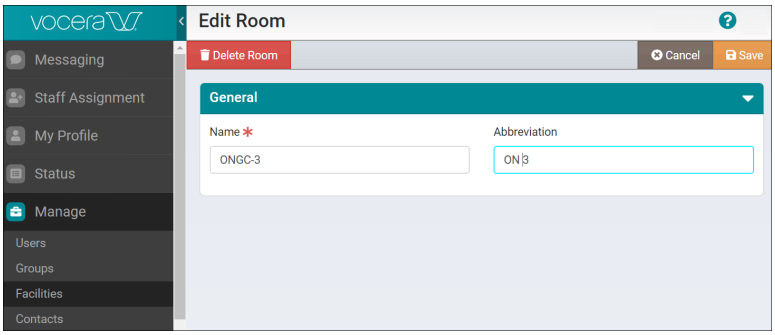
3. Select **Delete Room** in the dropdown menu.



   The Delete Room dialog box appears.
4. Select one of the following to close the dialog.
   - **Yes** — to delete the room from the system.
   - **No** — to return back to the All Rooms page without deleting this room.



5. (Optional) When editing a room, the delete function is also available in the Actions bar.

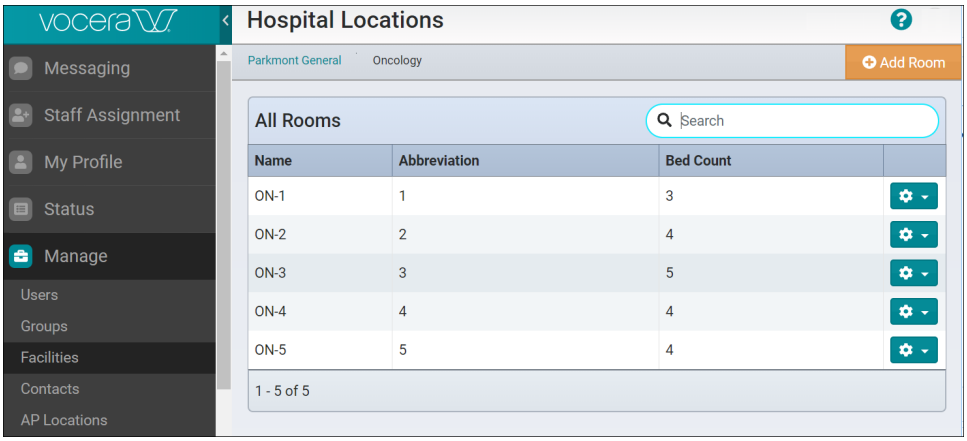


Working with Beds

You can view the beds that have been assigned for any rooms in a specific department.

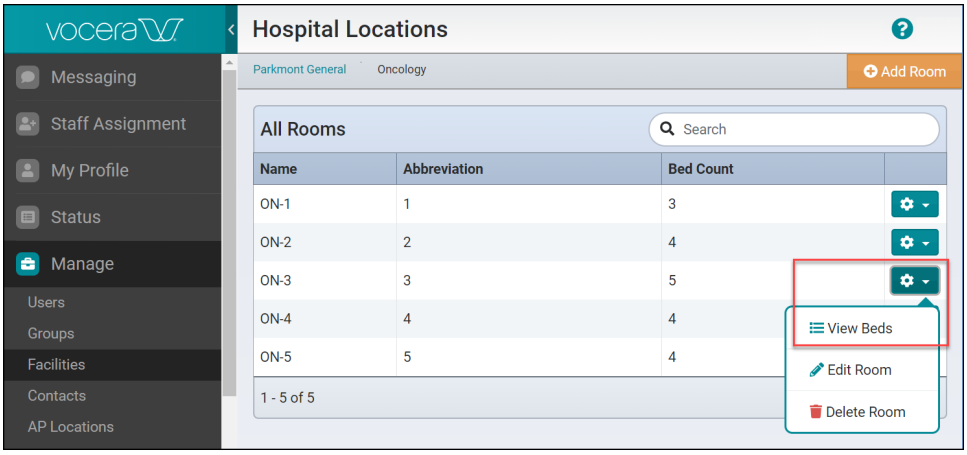
1. Navigate to the All Room page from a specific department as described in the Working with Rooms section.

   The All Rooms page displays the room names (in alphabetical order), an abbreviation for the room name, the bed count in each room, and an **Options** button.



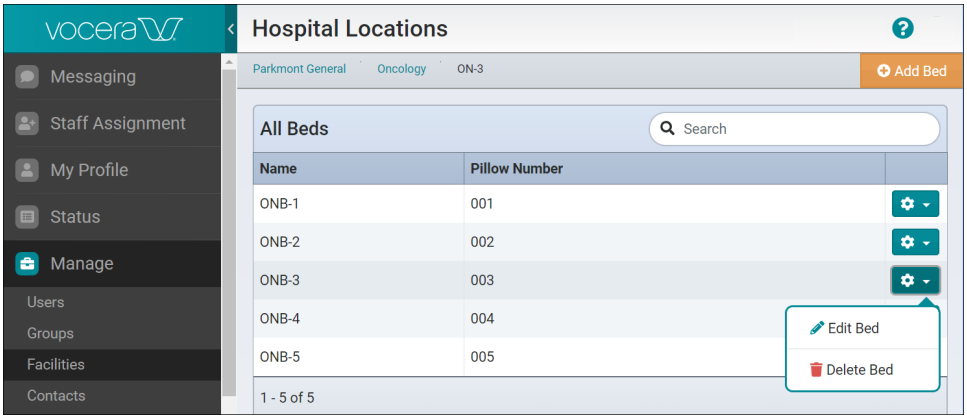
2. Click the **Options** button in the far right of this room's row.

3. Select **View Beds** from the Options dropdown menu.



The All Beds page appears with a list of beds assigned for this hospital room.

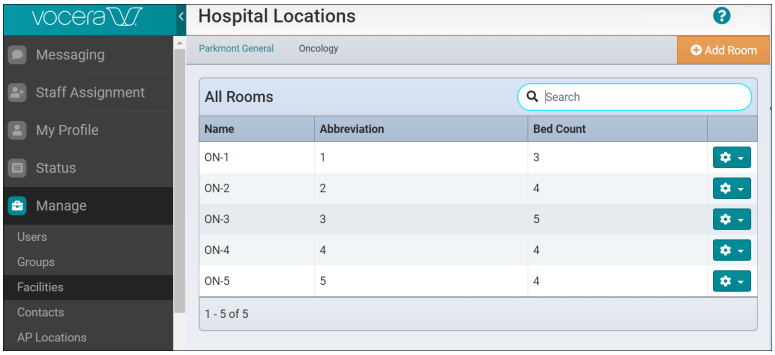
4. In the All Beds page, you can add, edit, or delete beds for the room.



Adding a Bed

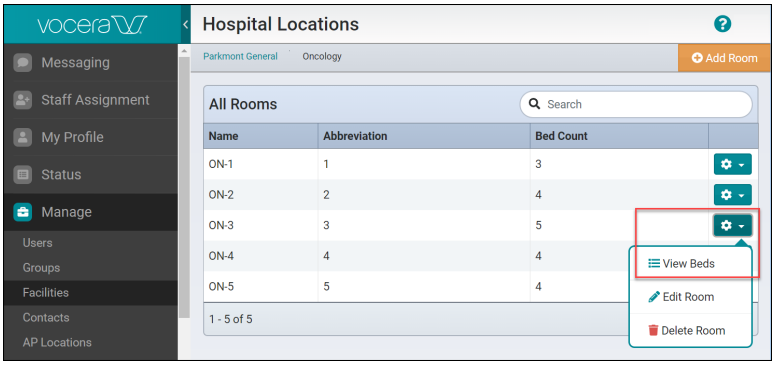
You can add a bed to any room that has been defined for a department in a hospital location.

1. Navigate to the facility, department, and room where you wish to work with beds. Verify the facility and unit in the breadcrumbs in the Actions bar.



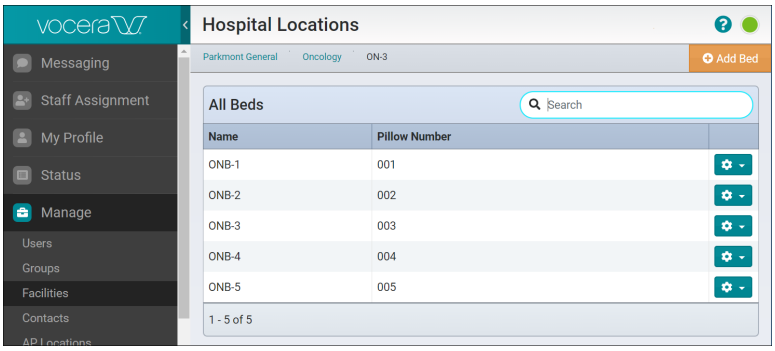
2. Click the **Options** button in the far right of this hospital room's row.

3. Select **View Beds** from the Options dropdown menu.



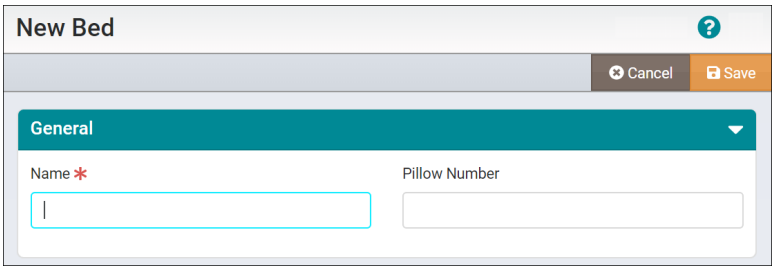
The All Beds page appears with a list of beds assigned for this hospital room.

4. Click **Add Bed** in the Actions bar.



The New Bed appears.

5. The New Bed screen contains two sections, Name and Pillow Number. Click the cursor in a field and start typing a new unit name.



6. Complete the fields listed in the table below. An asterisk * indicates that the field must be provided.

Name	Description
Name *	The name of the new bed.
Pillow Number	An optional pillow number to access the bedside phone.

7. Select one of the following to close the dialog.
   - **Save** — to add the new bed to the system.
   - **Cancel**— to return back to the All Beds page without adding a room.

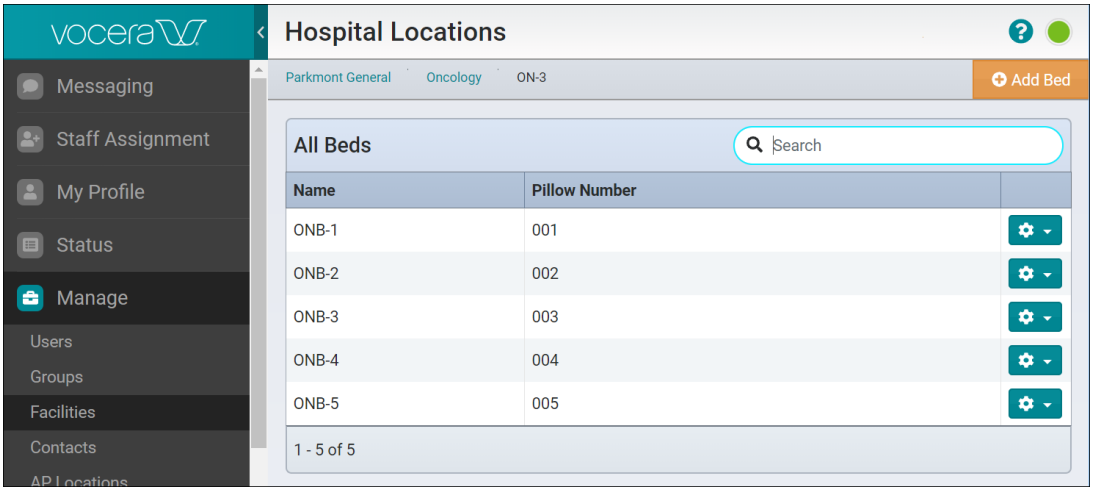
Editing a Bed

After you have created a bed in a room, you can edit the bed information.

Access the Vocera Platform Web Console to edit a bed in a room belonging to a unit in a Physical Location.

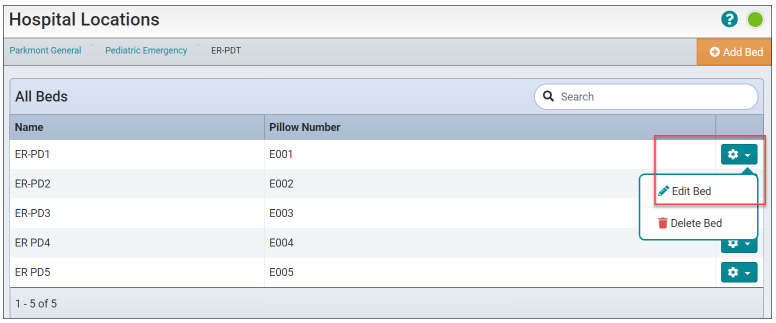
1. Navigate to the All Beds window to view the room where you wish to edit a bed. See Working with Beds on page 216.
   Verify the correct physical location in the Actions breadcrumbs.

The All Beds pane displays the bed names in numerical order, a pillow number (which is a number used to contact the phone at this bedside), and an Options button to access a navigation menu.



2. Click the **Options** button in the far right of this hospital room's row.

3. Select **Edit Bed** in the Options dropdown menu.



The Edit Bed page appears.

4. In the General section, enter a value for the fields listed in the table below.
   An asterisk * indicates that the field must be provided.

Name	Description
Name *	The name of the bed.
Pillow Number	An optional pillow number to access the bedside phone.

5. Select one of the following to close the dialog.
   - **Save**— to save the changes to the bed information in the system.
   - **Cancel**— to return back to the All Beds page without making any changes.

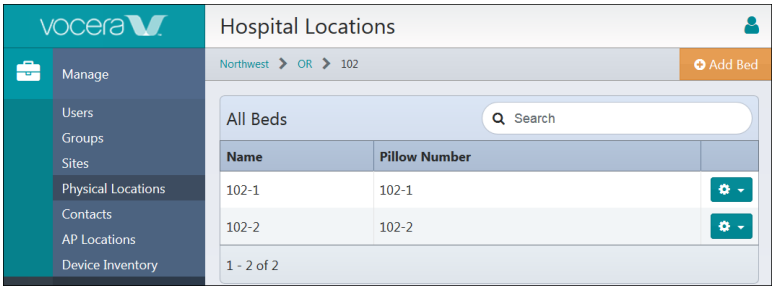
Deleting a Bed

You can delete a bed from a facility.

Access the Vocera Platform Web Console to delete a bed from a Physical Location.

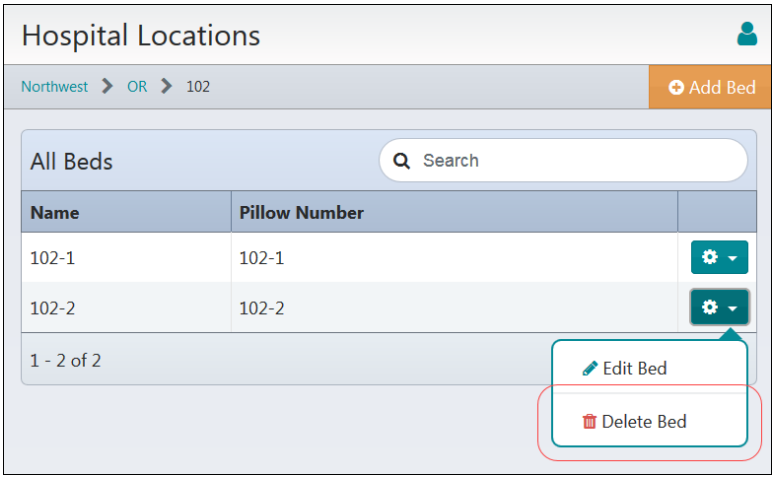
1. Navigate to the All Beds window to view the room where you wish to delete a bed. See Working with Beds on page 216.
   Verify the correct physical location in the Actions breadcrumbs.

The All Beds pane displays the bed names in numerical order, a pillow number (which is a number used to contact the phone at this bedside), and an Options button to access a navigation menu.



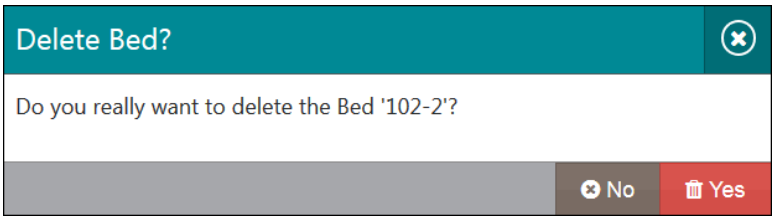
2. Click the **Options** button in the far right of the rooms's row that you wish to view.

3. Select **Delete Bed** in the Options popup menu.



The Delete Bed message window appears.

4. Select one of the following to close the dialog.
   - **Yes**— to delete the bed from the system.
   - **No**— to return back to the All Beds page without deleting a bed.



5. When editing a bed, the delete function is also available in the Actions bar.

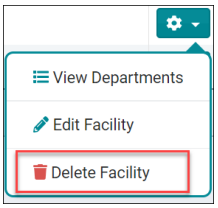
Deleting a Facility

You can delete an existing facility from the system, deleting a facility automatically removes the associated rooms and beds from the system.

You cannot delete the default Global facility.

1. Navigate to **Facilities** from the **Manage** section to locate the facility that you want to delete.
   The Hospital Locations page displays.
2. Navigate to the hospital location that you wish to delete in the alphabetical list under All Facilities.
3. Click the **Options** button in the far right of the hospital location's row.

4. Select **Delete Facility** from the Options drop down menu.



   The Delete Facility dialog displays.
5. Choose one of the following to close the Delete Facility dialog.
   - **No** — to cancel the delete action and return to the All Facilities page.
   - **Yes**— to confirm the delete action.

     Attention: The delete action permanently deletes a facility from the system. Deleting a facility deletes all users, groups, AP locations, devices, department, rooms, and beds associated with this facility.

Contacts

Contacts provide a way for Vocera users to save contact details of places and people who are not device users.

For example, if people in your organization frequently need to contact local businesses, you can enter the business names and nicknames in the Contacts list. Then, getting a price quotation from a local business named Northwestern Hardware becomes as simple as using a Vocera device to say “Call Northwestern.”

The distinction between whether a name is maintained in the Contacts list or in the user directory is usually transparent to device users. In either situation, device users can simply say, “Call Michelle Spangler” to reach the person they want to speak.

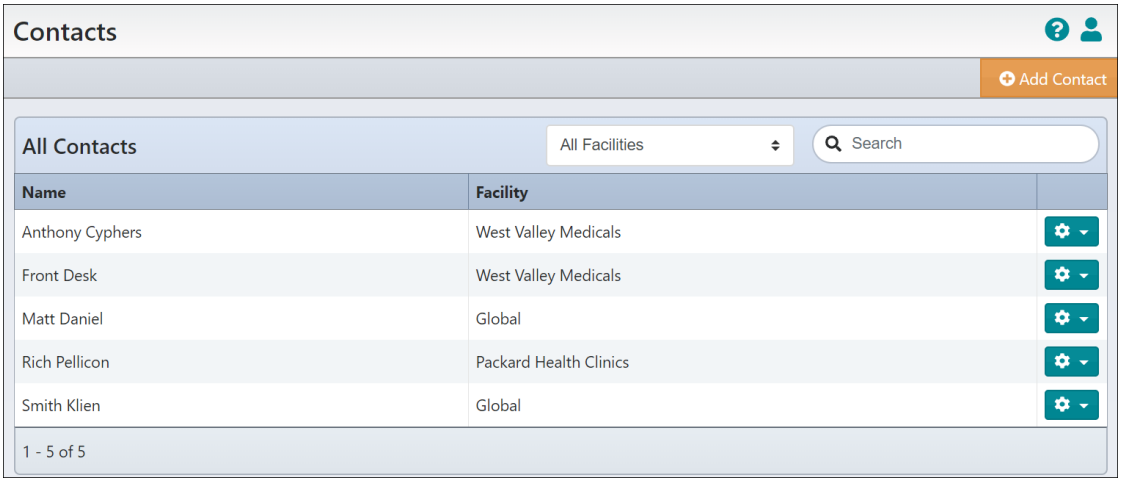
Contacts are available to anyone who has access to the Vocera system; they do not require permissions. For example, a user does not need the **Call Toll Numbers** permission to call a contact that you define with a toll phone number.

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 a contact, as well as a Vocera group or user.

You can use **Contacts** in the **Manage** section of the Vocera Platform Web Console to perform the following:

- View or Edit Existing Contacts
- Create New Contacts
- Search Contacts
- Sort Contacts
- Filter Contacts by Facility
- Delete Contacts

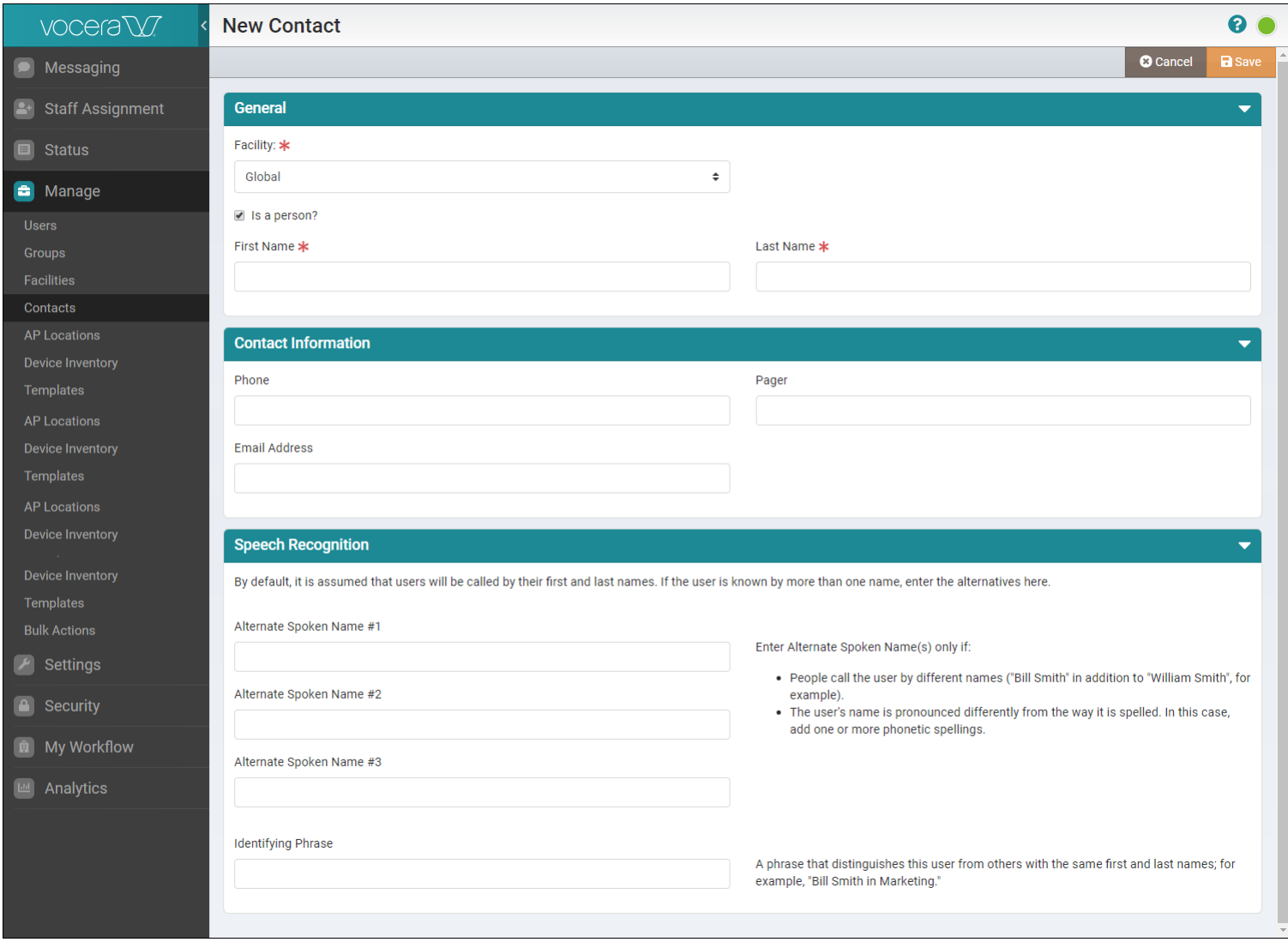
To view all the contacts in your system, select **Contacts** in the **Manage** section of the navigation bar. The Contacts page displays with a list of Contact Names and Facility information in an alphabetical order.



Adding a Contact

When you add a contact to your system you provide basic information to identify the entry, and contact information such as phone numbers and email addresses.

1. Navigate to **Contacts** in the **Manage** section, and click **Add Contact**.
   The New Contact page displays.



   The New Contact page includes the following three sections:
   - General
   - Contact Information
   - Speech Recognition

2. (Optional) Click the drop down arrowhead to expand a section and view the fields, then click the same arrowhead to collapse the section.
3. In the General section, complete the fields listed in the table below. An asterisk * indicates that a value must be entered for this field.

Field	Maximum Length	Description
Facility	N/A	Select the facility associated with your contact from the dropdown list. • If your organization has multiple facilities connected to the same Vocera Platform, choose the facility where users need to access this contact. If the entire organization uses this entry, choose the **Global** facility. • If your organization does not have multiple facilities, accept the default **Global** setting.
Is a person?	**N/A**	Select this checkbox if the new contact is a person, or clear the checkbox if the new contact is an organization. This checkbox is selected by default.
First Name *	**50**	If the new contact is a person, specify the first name of the contact. This field appears only if the **Is a person?** checkbox is selected. The value you provide in all name fields must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). No other characters are allowed. The speech recognition system uses the names you provide to recognize contacts.
Last Name *	**50**	If the new contact is a person, specify the last name of the contact. This field appears only if the **Is a person?** checkbox is selected.
Name *	**50**	If the new contact is an organization, specify the name of the organization. This field appears only if the **Is a person?** checkbox is cleared.

4. In the Contact Information section, complete the fields listed in the table below. You must complete at least one field if you want to reach a contact using a voice command.

Field	Maximum Length	Description
Phone	**50**	Specify the phone number for the new contact.
Pager	**50**	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 Contacts entry; when the recipient returns the call, it is connected directly to the user's badge.
Email Address	**60**	Enter an **Email Address** to allow users to send voice messages as an email attachment.

5. The Speech Recognition section lets you provide variations of a contact's name or identifying phrases to assist in speech recognition. Complete the fields listed in the table below.

Field	Maximum Length	Description
Alternate Spoken Names	**50**	Specify an alternate spoke name, you can add up to 3 alternate spoken names for a contact. Use these guidelines to ensure the best result when you are defining alternate names for users: • **Person, Group, and Location Names** — If users refer to a person, group, or location 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. • **Digits in Name Fields** — 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 these special characters are allowed, it is unlikely that an alternate spoken name would need underscores (_), or dashes (-). • **Staff IDs** — It is recommended that you do not create an alternate spoken name that contains numeric digits only. For example, a staff ID with numbers and no letters. `567748` Entering numeric staff IDs is permitted. However, using numeric values only might result in • Slower Genie response times • Problems with phone number recognition • **Acronyms and Initials in Alternate Spoken Names**— If people use an acronym or initials to refer to an entry in Contacts, 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. For Armandeep Munindar Gill, also enter A M Gill rather than A.M. Gill. • **Unusual Pronunciation**— If a name has an unusual or confusing pronunciation, or silent letters, 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. • **Professional Titles in Alternate Spoken Names**— If users refer to a person by his or her title, provide the full spelling of the title rather than an abbreviation. For example, enter Father Brown instead of Fr. Brown, or Professor Lindsay instead of Prof. Lindsay.
Identifying Phrase	**50**	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 they are in different departments, you could enter "Mary Hill in Pediatrics" as the identifying phrase for one user and "Mary Hill in Admissions" for the other.

6. Select one of the following to close the dialog:
   - **Save** — to add the new contact to the system.
   - **Cancel** — to return to the Contacts page.

Editing a Contact

Edit the information for an existing contact from the Vocera Platform Web Console.

1. Navigate to **Contacts** in the **Manage** section.
2. Locate the contact that you want to edit.
3. Choose one of the following:
   - Click on the name of the contact that you want to edit or click anywhere on the contact row to display the Edit Contact page.
   - Click the **Options** button in the far right of this contact.

1. Select **Edit Contact** from the dropdown menu in the **Options** button.
2. The Edit Contact page displays.

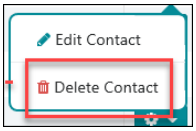
4. Edit the contact information as necessary. See Adding a Contact on page 223 for a list of the contact fields.
5. Select one of the following to close the dialog:
   - **Save** — to update the contact configuration changes.
   - **Cancel** — to return to the **Contacts** page.

Deleting a Contact

You can delete any existing contact from your list of contacts from the Vocera Platform Web Console.

1. Navigate to **Contacts** in the **Manage** section.
2. Locate the contact that you want to delete.
3. Click the **Options** button in the far right of the contact's row.

4. From the dropdown menu, select **Delete Contact**.



   The Delete Contact dialog box displays.
5. Choose one of the following to close the Delete Contact dialog box:
   - **No** — to confirm the delete action.
   - **Yes** — to cancel the delete action and return to the **Contacts** page.

About Contacts List for the Global Facility

If you have multiple facilities and have enabled telephony for the Global facility, you can use the Global Contacts list to store information for people and places that users from all facilities need to access.

Note: If you have not enabled telephony for the Global facility, you cannot make calls to Global contacts.

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

For example, suppose all the facilities 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 calling information in a contact; in addition, because users at any facility may need to call the wholesaler, its information belongs in the Contacts list for the Global facility.

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

Using Voice Commands with Contacts

Vocera device users can continue to use voice commands to reach contacts who are not using Vocera devices.

Device users can issue the following voice commands to reach contacts:

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

For guidelines on using voice commands, see the supported Device User Guide on the Vocera Devices page.

Using Macros in Contacts

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

It also provides examples of some other contacts that you may want to implement.

Calling Home

You can use the built-in dialing macros to create a single contact that any Vocera device 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 of the **Contact Information** section of the **New User** or **Edit User** page.

1. Create a contact as described in Adding a Contact on page 223.
2. Make sure the **Is it a person?** field is not selected.
3. In the **Name** field, enter a name such as **My House**. Make sure you use at least two words in the name for optimal speech recognition.

   Do not use the name “My Home” for this contact. Device users can issue the command “Forward calls to my home phone” to forward calls when they are away from their facility. If users instead accidentally forward calls to the contact called “My Home”, other badge users who call them will experience unexpected results. Users should not forward calls to a contact that evaluates to the **%H** macro.
4. Enter **%H** in one of the **Phone** fields.
5. 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 a contact for a place.

For example, call it `Night Bell` or `After Hours` — and enter the code in one of the **Phone** fields.

Access Point (AP) Locations

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

When a device connects to an access point, the Vocera Platform is able to report the name of the corresponding location.

You can use the Vocera Platform Web Console to view and manage the access point locations created on your system.

When AP locations is entered in the system, device users can use "Locate", "Where Is?", and "Where Am I?" voice commands to find the physical location of a particular user or member of a group within a facility.

If you configure AP Locations for your system, the Genie can respond with information about a user's whereabouts. For example, "Roswell Adams is near the First Floor Cafeteria". If you do not configure an AP Location, the Genie responds with the MAC address of the access point instead, which is not useful to most device users. For example, when a device user says, "Locate *Lucy Crysek*." Genie may say, "Lucy Crysek is near access point zero zero four zero nine six four five B D four E."

For guidelines on using the voice commands, see your supported Vocera Device User Guide on the Vocera Devices page.

Important: By default, every access point on your network is associated with the Global facility. If your deployment involves multiple facilities, assign a location name to each access point, and associate each of these locations with a facility. Otherwise, the Vocera Platform assumes that the default Global facility is your current facility.

Keep in mind that Vocera devices, like all wireless devices, do not always associate with the access point that is physically closest. A device may associate with an access point situated on a different floor, depending upon building construction. The device can only offer approximate user locations; consequently, generic location names may be more useful than specific ones.

Defining Locations

Well defined access point location minimize the effects of signal retention.

When you define locations, start with a map of the facility and note where the access points are installed. (This may already have been done as part of the facility 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 Vocera Platform Web Console.

Location information will be most accurate if you draw the boundaries around sizeable, contiguous areas. Vocera devices, 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.

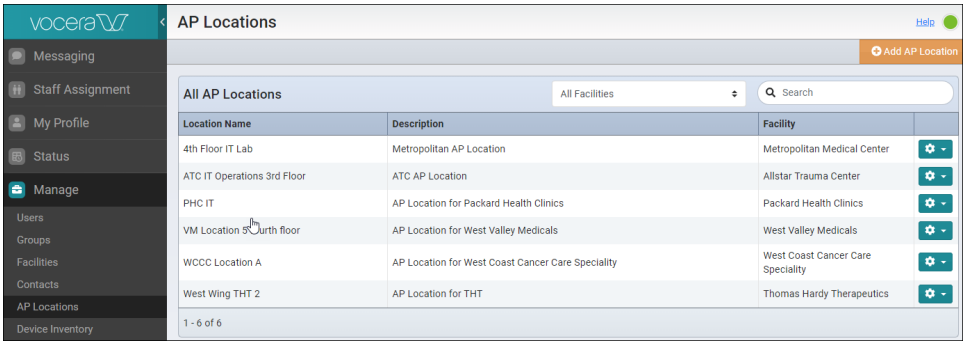
After you create the location map, you can add locations and choose their neighbors in the Vocera Vocera Platform Web Console. Then you can record a name prompt for each location. (See Recording a Location Name on page 232.)

Managing Access Point Locations

View and manage the access point (AP) locations created on your system.

When a Vocera device connects to an access point, the server is able to report the corresponding location.

To view all the AP locations in your system, select **AP Locations** from the **Manage** section of the navigation bar. The AP Locations page displays with a list of AP locations in alphabetical order.

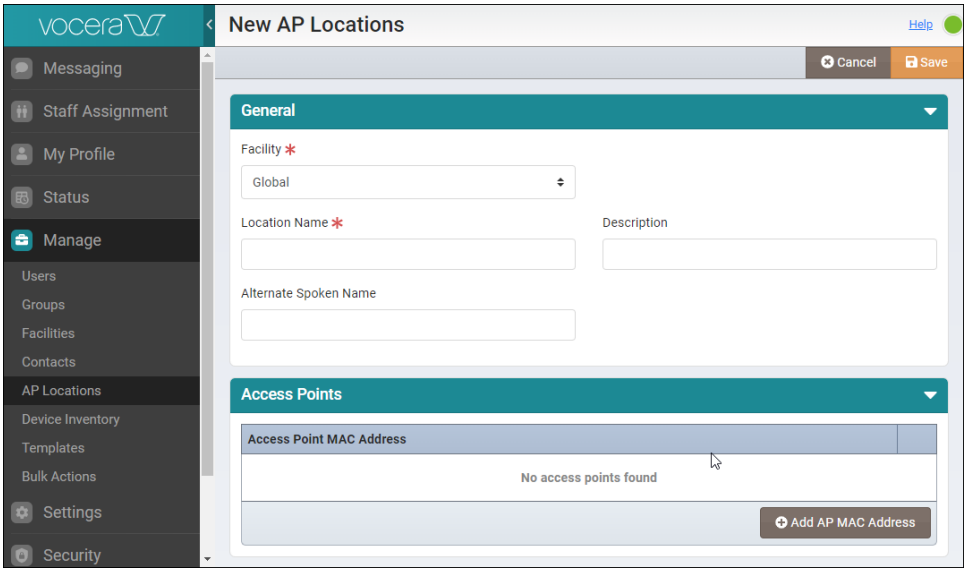


From the **AP Locations** page you can add, edit or delete an access point.

Adding an Access Point Location

You can add a new access point (AP) location to the list of access point locations.

1. Navigate to **AP Locations** in the **Manage** section.
2. Select **Add AP Location** in the menu to display the New AP Locations page.



The **New AP Locations** page has two sections:

- General
- Access Points

Tip: You can click the drop down arrow at the right hand side of each section to expand or collapse these sections.

3. In the General section, complete the fields listed in the table below. An asterisk * indicates that a value must be entered for this field.

Field	Maximum Length	Description
Facility *	100	Use the **Facility** drop down list to select the physical location of the access point. • If your organization has multiple locations connected to the same Vocera Platform, choose the facility that represents the access point's physical location. • If your organization does not have multiple facilities, accept the default **Global** setting.
Location Name *	50	The name of the location. 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	(Optional) Enter a **Description** to identify the location.
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 (for example, "Locate members of managers closest to the first floor"), the Vocera Platform 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. For example, if the Administration Building is often called the Clock Tower Building, enter Clock Tower Building. The Alternate Spoken Location Name gives the server an additional field to check, increasing the chances of Genie's ability to understand the location name correctly.

4. In the Access Points section, add or delete the access point MAC addresses for a location.

   To add a MAC address:

   1. Click **Add AP MAC Address** to display the Add AP MAC Address dialog box.
   2. In the AP MAC Address field, enter the MAC address (12 hexadecimal characters) of an access point that you want to assign to this location.

      Tip: 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 wild card only in the 12th character of the MAC address.

   3. Click **Done**, and the MAC address will appear in the list of access point MAC addresses.

   To delete a MAC address:

   1. Choose a MAC address from the Access Point Addresses.
   2. Click **Delete**.

5. Select one of the following to close the dialog:
   - **Save** — to add the access point location to the system.
   - **Cancel** — to return to the AP Locations page without adding an AP Location.

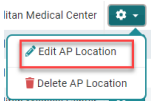
Editing an Access Point Location

You can edit the information for any existing access point location.

1. Navigate to **AP Locations** in the **Manage** section.

2. Locate the access point location that you want to edit.
3. Choose one of the following:
   - Click on the AP Location name that you want to edit or click anywhere in the Access Point Location row to display the Edit Access Point Location page.
   - Click the **Options** button in the far right of this AP Location.

     1. Select **Edit** from the drop down menu in the **Options** button.

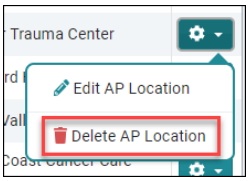
     2. The Edit AP Location page displays.
4. Edit the access point location information as necessary. See Adding an Access Point Location on page 229 for a list of the access point location fields.
5. Select one of the following to close the dialog:
   - **Save** — to update the configuration changes.
   - **Cancel** — to return to AP Locations page.

Deleting an Access Point Location

You can delete any existing access point location from the Vocera Platform Web Console.

1. Navigate to **AP Locations** in the **Manage** section to locate the AP Location that you want to delete.
2. Click the **Options** button in the far right of the access point location that you want to delete.

3. Select **Delete AP Location** from the drop down menu in the **Options** button.

   The system displays a confirmation message to confirm if you really want to delete the selected AP Location.
4. Choose one of the following to close the dialog:
   - **Yes** — to confirm the delete action.
   - **No** — to cancel the delete action and return to the AP Location page.

Searching for AP Locations

You can filter search results based on location names, descriptions, and MAC address field values.

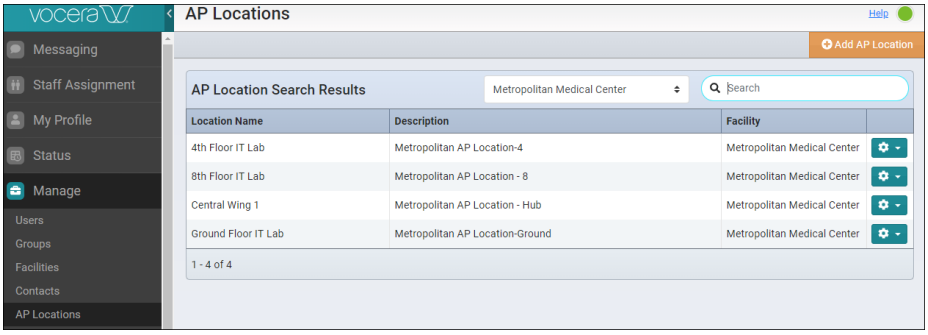
The Search feature in Vocera Platform Web Console is especially helpful in large deployments with multiple facilities and multiple access point locations.

You can refine your search to view results based on the values you entered for the location name, description, and MAC address fields of an AP Location. Similarly, you can use the same criteria to search for AP locations within a specific facility.

Use one of the following ways to search for AP Locations:

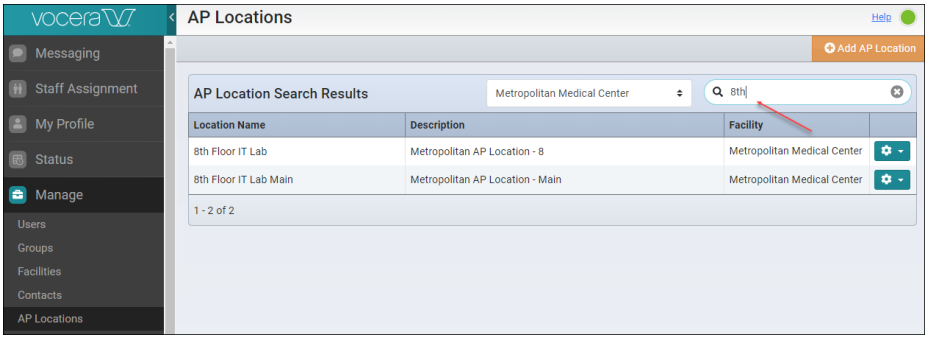
- Enter a character for Location Name or Description field values in the Search field to display search results on all AP Locations in all facilities.
- Enter a MAC address in the Search field to find an AP location that contains this MAC address value.
- Toggle the Facility selector in the Action bar to sort and display a list of AP Locations associated with a specific facility.

  For example, if you toggled the Facility selector and chose a facility named “Metropolitan Medical Center”, the Search feature will display results for all AP Locations in this Facility.



- Toggle the Facility selector to select a specific facility and enter a character to search AP Locations based on Location Name, Description, or the MAC address value.

  For example, if you selected a facility named, “Metropolitan Medical Center”, and start typing, “8th” in the Search bar. The AP Location Search Result displays all AP Location records matching this information, as shown in the following screenshot.



Recording a Location Name

Record a location name prompt to avoid potential mispronunciations.

After you assign location names to access points, you can use the location names with voice commands. For example, “Find a member of nurses close to the E R”, and the Genie responds with location names when appropriate “Mary Smith is near the Main Desk”. If you record location names with your natural voice, you can avoid potential mispronunciations caused by the synthesized pronunciations.

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 device as a user with system administration privileges.
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 facilities, users, groups, locations, and contact entries have the same name or alternate spoken name, you can record a name prompt for only one of them.

Using Voice Commands to Assign Access Points

You can use the, “Begin Tour”, “End Tour”, and “Assign Location” voice commands to assign specific access points.

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.
- Make sure you are logged in to your device as a member of a group with permissions to perform system administration tasks.
- Make sure you are at your home facility. You can use voice commands on a Vocera device to assign access points to locations only when you are at your home facility.

For guidelines on using voice commands, see the supported Device User Guide on the Vocera Devices page.

1. Using a Vocera device, 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 Platform is still monitoring your movements over the wireless network, however.
3. Begin walking slowly through the area covered by your network. Each time your device 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 Vocera Platform Web 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.”

What to do next:

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" voice command.

Device Inventory

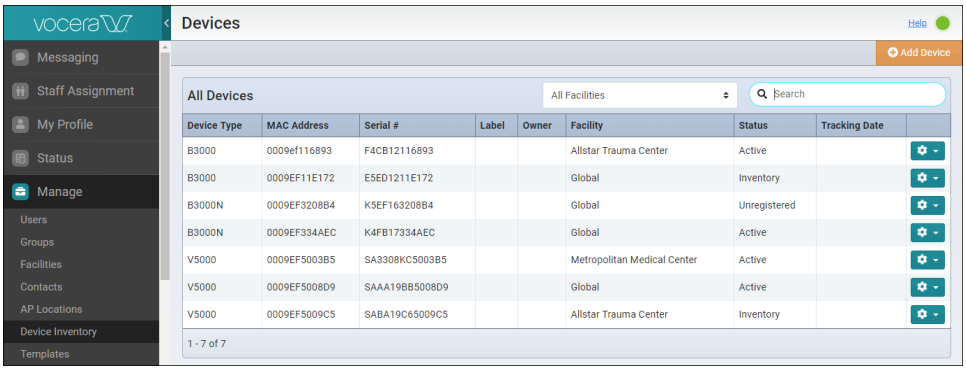
Device Inventory provides a way to manage, track, and maintain the hardware devices that connect to the Vocera Platform.

You can use the device inventory information to perform the following tasks:

- 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

The **Device Inventory** in the **Manage** section of the Vocera Platform Web Console lets you view and manage the devices that are in use on your system.

You can add, edit, or delete a device from the **Devices Inventory** section in the Web Console. By default, the **Devices** page displays all devices currently in the Vocera system.



Note: 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. See Device Management Roles to understand these roles and their responsibilities.

Adding a Device

Add a Vocera device with information that lets you identify, monitor, and track a device in your system.

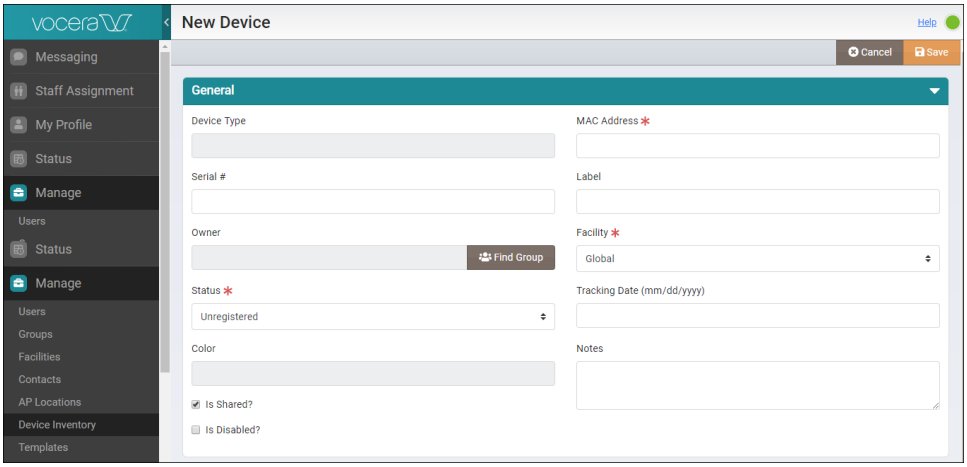
As soon as a Vocera device arrives at a facility, enter its identifying information into the Vocera system so you can track and monitor it appropriately. Do this right away, even before the device is configured; it helps prevent the device from being lost or transferred to another department. It also allows you to monitor and report on the device status.

You can add devices to the Vocera system in any of the following ways:

- Load devices automatically when they connect to the Vocera Platform. See Automatically Loading Devices into the System on page 245.
- Add devices manually using the **Device Inventory** in the **Manage** section of the Vocera Platform Web Console.

Note: You must have system administrator or system device manager permissions to add devices manually. Group device managers cannot use the Vocera Platform Web Console to add devices.

1. Navigate to **Device Inventory** in the **Manage** section of the navigation bar.
   The **Devices** page appears.
2. Click **Add Device** to add information for a new device.
   The **New Device** page appears.



3. In the **General** section, complete the fields listed in the table below. An asterisk * indicates that you must provide a value for the field.

Field	Maximum Length	Description
Device Type	n/a	This read-only field specifies the type of device, which is determined from the serial number. Device types include B3000, B3000n, V5000, Smartphone, Apple, and Android.
MAC Address *	12	Specifies the MAC address of the device in hexadecimal characters. For Vocera devices, 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. To learn more about the MAC Addresses, see About Serial Numbers and MAC Addresses.
Serial #	15	Specify the serial number of the device. For Vocera devices, the serial number is 12 characters. For Vocera Smartphones, the serial number is 10 characters. To learn more about the Serial numbers, see About Serial Numbers and MAC Addresses
Label	20	Specify a label that uniquely identifies the device. For more information, see Labeling Devices on page 246.
Owner	n/a	Specify the group that owns the device. Click the **Find Group** button to open the Find a Group dialog box, then choose a group from the list and click **Select Group**. The facility of the group that owns a device can be different from the facility of the device itself.

Field	Maximum Length	Description
Facility	n/a	Specify the device's home facility. Click the drop down arrow to view the available facilities, and then scroll down to select a facility of your choice. • If your organization has multiple facilities connected to the same Vocera Platform, choose the home facility that represents the device's physical location. • If your organization does not have multiple facilities, accept the default **Global** setting. **Note:** When working with the data-loading template available in Bulk Actions, leave this field blank to accept **Global**. For more information on data-loading templates, see Bulk Actions on page 254 .
Status *	n/a	Select the device status from the dropdown list. If you have System Administrator permission, you can select a new status from the available list of status. See Viewing Device Information Statuses on page 286 for more information.
Tracking Date	n/a	Specify a date to track the device. For example, you can track when the device was sent for repair or return merchandise authorization (RMA). Click in the space provided next to the **Tracking Date** field to enter a date. A calendar pop-up for the current month is displayed. You can select the current date from this calendar.
Color	n/a	This read-only field specifies the color of the device, which is determined from the serial number. Vocera devices are either white or black.
Is Shared?	n/a	Uncheck this box to indicate that multiple users don't share this device. The **Is Shared?** checkbox is selected by default.
Is Disabled?	n/a	Check this box to disable the device. If the device is disabled and the **Call** button is pressed, the Genie plays the following prompt, "This device has been disabled, please contact your administrator. " Upon hearing this prompt, the user can return the device to prevent inventory loss. **Note:** If you disable a device, and a user is logged into this device at that time, they are logged out immediately.
Notes	1000	Optionally, specify a multi-line text box that lets you provide further information about the device status. For example, "Device stopped working on [DATE] after accidentally being immersed in water" or "Device sent to IT to repair the battery latch."

To ensure the accuracy of serial numbers and MAC addresses, you can use a bar code scanner to scan device labels or inventory sheets. For more information, see Using a Barcode Scanner to Add Devices on page 243.

4. Select one of the following to close the New Device page:
   - **Save** — to add the new device to the system.
   - **Cancel** — to return to the Devices page.

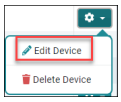
Editing a Device

You can edit the information for an existing device.

1. Navigate to **Device Inventory** in the **Manage** section.
   The Devices screen displays a list of devices in your system.
2. Locate the device that you want to edit.
3. Choose one of the following:

- Click on any fields displayed in the Device Table for the device that you want to edit. The Edit Device page is displayed.
- Click the **Options** button in the far right of this group.

1. Select **Edit Device** from the drop down menu in the **Options** button.



2. The Edit Device page displays.

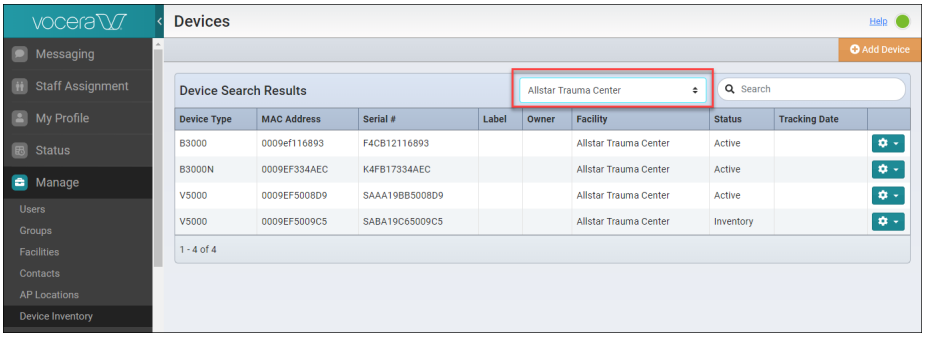
4. Edit the device information as necessary. See Adding a Device on page 234 for a list of the device fields.
5. Choose one of the following to close the dialog:
   - **Save** — to update the device configuration changes.
   - **Cancel** — to return to the Devices page.
   - **Delete Device** — to remove the device from the system permanently.

Filtering Devices by Facility

Filter and view devices in a specific facility.

By default, the Web Console displays devices for all facilities in the system.

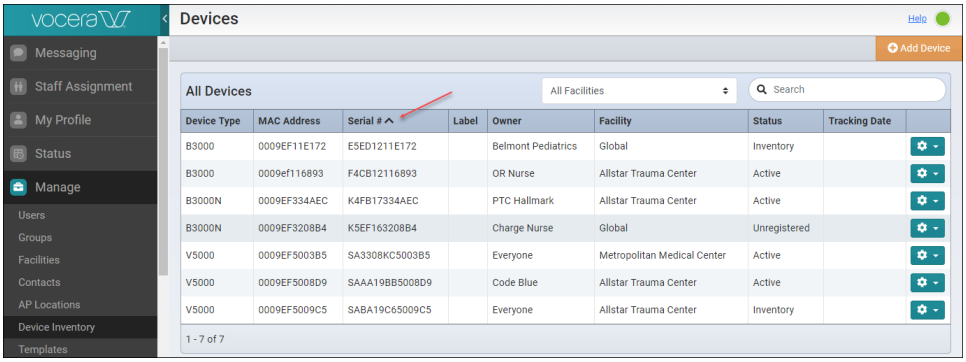
1. Navigate to **Device Inventory** in the **Manage** section
   The Devices page displays with a list of all devices in the system.
2. Toggle the **Facility** selector in the Action bar to sort and display a list of devices associated with a specific facility.
   The search immediately pulls any records matching this information and displays all devices in the Device Search Results.
   For example, if your system has a facility named “Allstar Trauma Center” you can select this facility's name in the Facility selector to display all devices in this facility.



Sorting Devices

You can sort the Devices table by any one of the columns.

For example, to sort by serial number, click the **Serial #** column heading as shown in the following screenshot.



Similarly, you can sort by **Device Type**, **MAC Address**, **Label**, **Owner**, **Facility**, **Status**, or **Tracking Date** columns.

You can sort by only one column at a time.

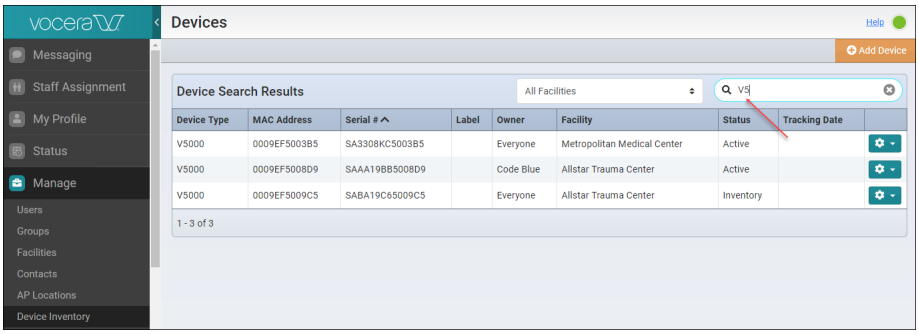
Searching for Devices

You can search for a device by its MAC address, serial number, label, owning group, device status, or tracking date.

Finding a device is easy. As you start entering characters in the **Search** bar, search filters matching device entries and display a list

You can also select a specific facility from the **All Facilities** dropdown to search for devices in a specific facility.

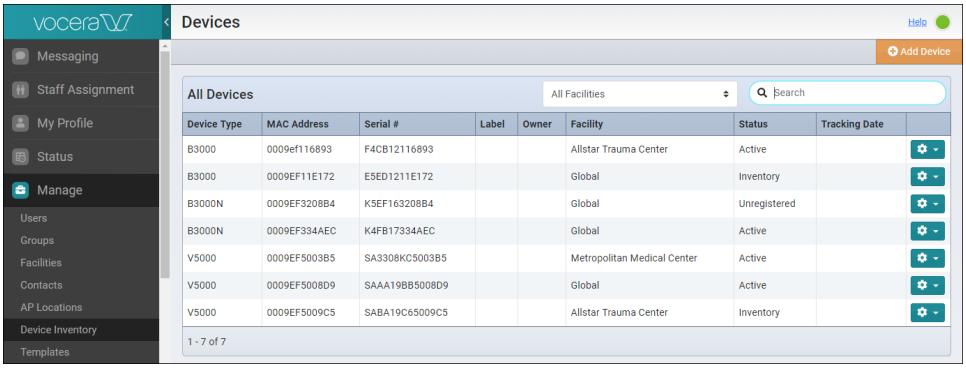
The following screen shot shows search results from a search entry based on the first two letters, “V5” for the Device Type: V5000.



Viewing Devices

Use the Vocera Platform Web Console to view and manage the devices that are in use on your system.

Select **Manage > Device Inventory** in the navigation to display the **Devices** page. From the **Devices** page, you can add, edit, or delete a device. By default, the **Devices** page displays 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.



Deleting a Device

You can delete records for devices with a wrong serial number or MAC address information in the system.

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 continues to appear in device management reports.

Note: Do not delete an active device. If you delete a device that is still in use, it is automatically added again to the system the next time it connects to the server.

1. Navigate to **Device Inventory** in the **Manage** section.
   The Devices page appears.
2. Locate the device that you want to delete. In the far right of this device's row, click the **Options** button:

3. Select **Delete Device** from the drop down menu.
4. Choose one of the following to close the Delete Devices dialog box:
   - **Yes** — to confirm the delete action.
   - **No** — to cancel the delete action and return to the **Devices** page.

Device Management Guidelines

To get the most value from your device management system, ensure that you define, document, and approve processes. Also, appoint administrators or managers and train your staff properly.

Enterprise Guidelines

Identify a staff member to oversee the Vocera system device management process.

- If your enterprise is large or has multiple facilities, you may want to have multiple Vocera system device managers.
  For a description of system device manager responsibilities, see Device Management Roles on page 240.

- 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 Platform Web 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.

Group Guidelines

For each group deploying Vocera, identify a staff member who can oversee the Vocera group device management process.

- For a description of group device manager responsibilities, see Device Management Roles on page 240.
- Develop and document group 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 Vocera Platform Web Console to edit device information, as well as monitor active devices. Also, train the group device managers on viewing and analyzing device management and speech recognition reports.

Managing Shared Devices

Vocera devices are often shared between multiple users rather than being assigned to a single user to reduce the total cost of hardware.

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 **Is Shared?** box is selected when you add each device into the Vocera system.
- Make sure the label on a shared device indicates the owning group instead of an individual user.
- Make sure the shared devices are not lost, use the Vocera Report Server or Vocera Analytics to track shared devices.

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 device management roles:

Role	Permissions Required	Description
System Administrator	Perform System Administration	Individuals with full permissions for adding, editing, and deleting data in the Web 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.
System Device Manager	Perform System Device Management	Individuals with tiered administrator access to the **Device Monitor** and **Device Inventory** sections of the Web Console, with full permission to add, edit, and delete device data, including device status values, for all facilities. To define which users are system device managers, the system administrator should create a group. For example, "Tiered Admin-Perform System Device Management," and grant the group the device management permission, and populate it with members who are system device managers. 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 facility may have a Vocera system device manager or a single person may manage Vocera devices for all facilities.
Group Device Manager	none	Individuals who can manage devices owned by groups. Group device managers can access the **Device Monitor** and **Device Inventory** sections of the Web 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.

If you are a user with any of device management roles mentioned in the table, you may want to learn more about theWeb Console Device Monitor.

System Device Manager Responsibilities

A quick summary of the responsibilities of an individual in the System Device Manager role.

- 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

A quick summary of the responsibilities of an individual in the Group Device Manager role.

- 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

A quick summary of the capabilities of both the Group and System Device Manager roles is described in the following table.

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)

About Serial Numbers and MAC Addresses

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 device, the MAC Address field is populated automatically. The length of serial numbers varies per device type. The following table lists Vocera devices with the serial number length for each device:

Device Type	Serial Number Length
V5000 Smartbadge	14
B3000n	12
B3000	12
Smartphone	10
Cisco Unified Wireless IP Phone 7921G, 7925G, and 7926G	12

Most MAC addresses for Vocera devices 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 the Vocera devices.

When you add or update a Vocera device, 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 device serial number without a MAC address, the system automatically fills in the value, whether you are using the Web Console to add or update the device or are importing the data from a CSV file.

Using a Barcode Scanner to Add Devices

The back of each Vocera device has a label that includes barcodes for the serial number and MAC address of the device.

In addition, an inventory sheet with barcodes of the devices' serial numbers is included with every Vocera device pack. You can use a handheld barcode scanner to scan the device 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 devices from Vocera, it is much easier to scan barcodes for the device serial numbers from the inventory sheet that accompanies the Vocera device pack. The inventory sheet includes barcodes for the serial numbers of all devices packed in the box.

The following figure shows a user scanning barcodes from a Vocera inventory sheet.

Individual devices 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 device clamshell.

The following figure shows a user scanning the barcode label on the back of a Vocera device.

For information on adding devices using a barcode scanner, see Adding devices Using a Barcode Scanner .

Tips for Scanning Devices

This topic summarizes the best practice guidelines for scanning barcode labels on Vocera devices.

- Hold the device at a standard reading distance from the scanner. The standard reading distance varies depending on your scanner model. For some scanners, the standard 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 Device dialog box. If you scan the MAC address barcode first, the **Serial Number** field is populated with the MAC address, and the record is therefore invalid.
- If you are scanning a Vocera badge, scan only the serial number. The MAC address field is populated automatically.

Barcode Scanner Requirements

When you scan Vocera barcodes, you must use a scanner capable of reading and scanning **Code 128** barcodes.

Many scanners read and scan Code 128 barcodes by default. If your scanner, does not do this by default, you can configure it 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.

Adding Devices Using a Barcode Scanner

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 244.
2. Obtain either the devices or inventory sheets for the devices you need to scan.
3. Log in to the Vocera Platform Web Console, and click **Devices** in the **Manage** section of the navigation bar
4. Click **Add Device**.
   The New Device dialog box appears.
5. Specify the common values for the Add Device dialog box that are shared between all devices you are scanning.
   - If the devices share the same **Tracking Date, Owner,** and **Facility,** specify values for those fields. Otherwise, leave them blank for now and fill these fields later.
   - If you are assigning the devices to a group, change the status from "Unregistered" to "Inventory" or "Active."
   - If multiple users in a group share the devices, make sure to check the **Shared Device?** box.

   Important: These values are used for all of the devices that you scan during the session.
6. Click the **Serial Number** field.
7. 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.

   Once the **Serial Number** and **MAC Address** fields are completed, the device is saved automatically after a brief pause. The Add Device dialog box remains open, and the **Serial Number** and **MAC Address** fields are cleared so that you can add another device.

Automatically Loading Devices into the System

Vocera automatically loads new devices into the system the first time you connect to the Vocera Platform.

This feature ensures that every device that connects to the Vocera Platform 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
- Facility
- Type
- Color

By default, the status given to devices automatically loaded by the server is “Unregistered.” The system device manager should use the **Devices** section in the Web Console to assign unregistered devices to an owning group and change the status from “Unregistered” to “Inventory” or “Active.” See Adding a Device Status on page 288 and Editing a Device Status on page 288 for more information.

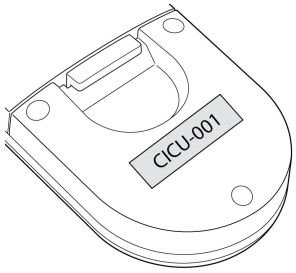
Labeling Devices

The label is the most important field for a device because it uniquely identifies the device by associating it with a group, department, 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 vital for loss prevention; the label 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 Web 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 the 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 back of a badge, beneath the battery compartment.



- 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

System device managers, group device managers, and system administrators can use the Device Monitor section of the Vocera Platform Web Console to monitor all active devices on the system.

After a device has been added to the system and assigned to a group, the device activities are displayed in the Device Monitor section. See Device Monitor for more information.

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 Monitor** section of the Vocera Platform Web Console.

Reporting on Devices

Vocera Analytics provides asset tracking reports or dashboards that show which users or departments are using Vocera devices and the type of devices that are in use.

These reports and dashboards can help you view device inventory, find missing devices, identify non-functioning devices, and plan for department needs based on usage patterns. For more detailed information about these reports and dashboards, see the Vocera Report Gallery User Guide and the Vocera Analytics Gallery User Guide

Device Management Licensing

If you have a Vocera Enterprise License, Vocera device management features are included with your license.

The Vocera device management features include the asset tracking capabilities of both the Vocera Report Server and Vocera Analytics.

If you have a Vocera Standard License, there is an additional charge for Vocera Report Server or Vocera Analytics software and Device Management.

Contact Vocera Customer Support to upgrade your Vocera license.

Templates

Create easy-to-use templates to deliver quick notifications regarding an important or a standard event.

Templates allow you to populate clear and concise messages for standard communication procedures or a critical event notification. A template is created with multiple fields in a pre-populated form so that it is easier for a designated user to send this template based event notification to recipients quickly.

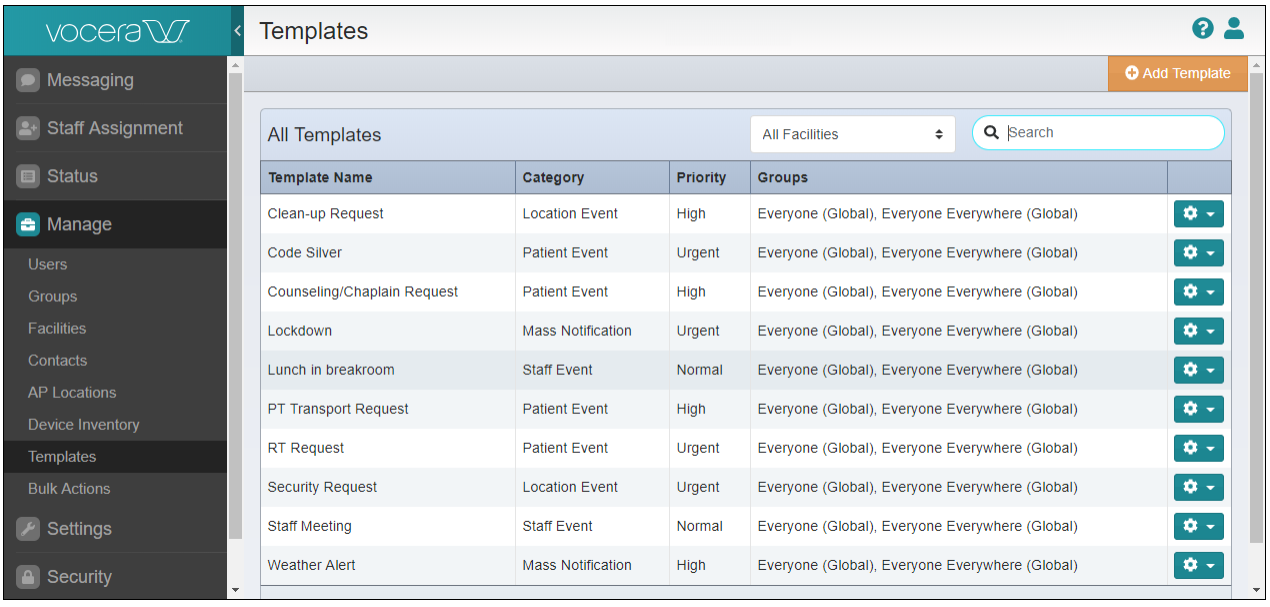
As a system administrator, you can create customized templates for your department or facility and designate specific users or members of a group to send the templates out to recipients (for example, care team members or staff members) so that they can receive these event notifications and respond to them quickly.

For example, in emergencies like a Code Blue event, where a patient had a cardiac arrest and the care team is required immediately to help in resuscitating or reviving the patient, system administrators can create a code-blue template ahead of time with several pre-populated fields and save it in the system. Designated users can immediately search for the existing code-blue template and send it out without worrying about filling all the required fields in the form.

Similarly, you can also use a pre-defined template for routine tasks. For example, you can create a template to request housekeeping for a patient's room or making a Staff Assist request for a specific patient and save these templates in the system for future use.

System administrators can create several such templates and let designated users send out such template based event notifications and also cancel them out when needed.

To create and manage your templates from the Vocera Platform Web Console, select **Templates** in the **Manage** section of the navigation bar. The list of available templates is displayed on the **Templates** page.

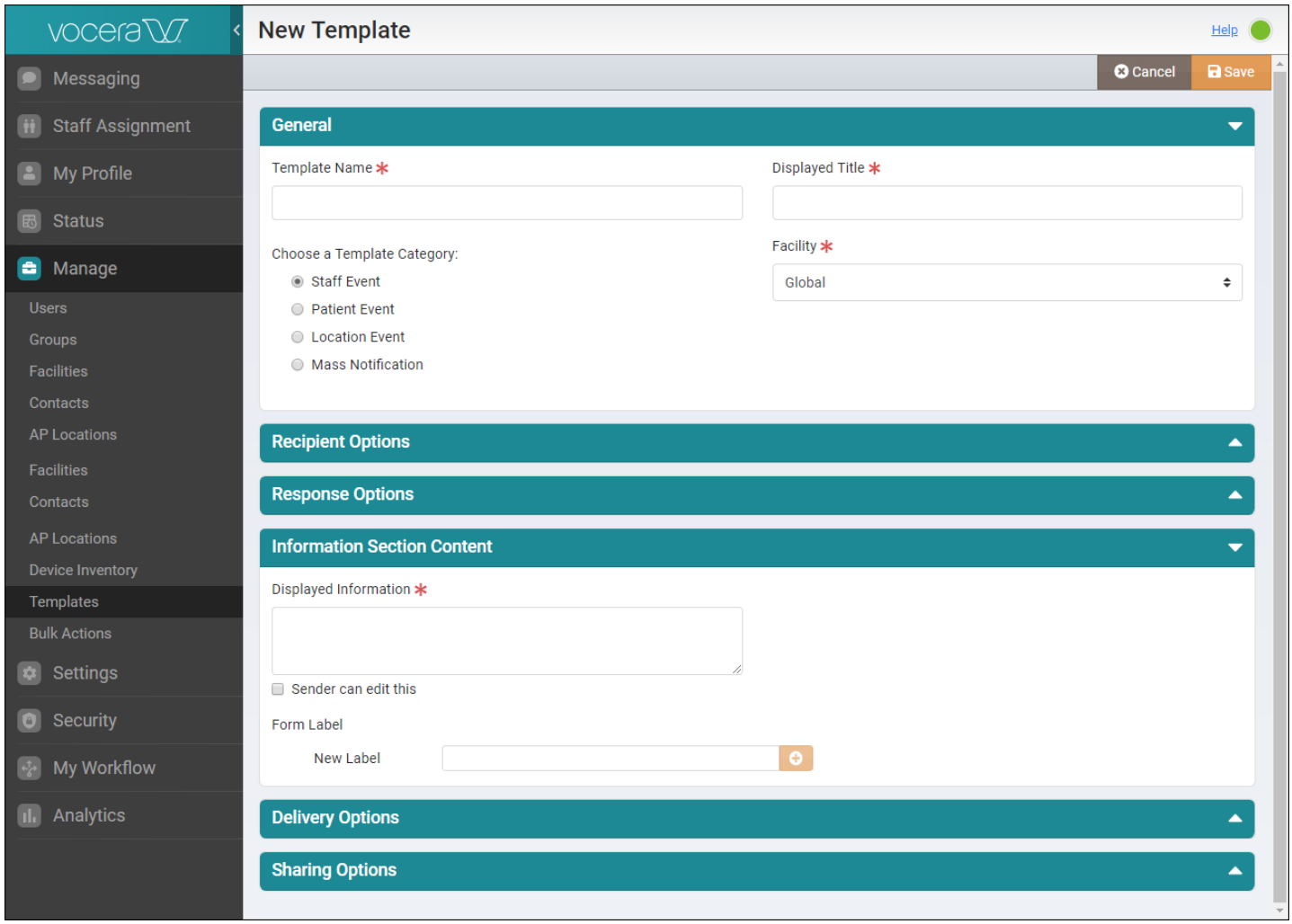


Adding a Template

You can add a template to the Vocera Platform Web Console list of templates and specify this template for a specific list of users.

When you create a Template, you can specify the list of groups, the message text, and priority. You can also supply a list of multiple-choice responses for recipients to choose from.

1. Select **Templates** in the **Manage** section of the navigation bar, and click the **Add Template** button. The New Template page displays.



The New Templates page has five sections:

- General
- Recipient Options
- Response Options
- Information Section Content
- Delivery Options
- Sharing Options

2. In the General section, complete the fields listed in the table below. An asterisk * indicates that you must provide a value for this field.

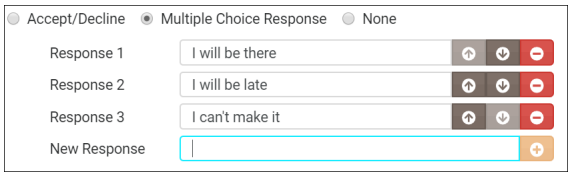
Field	Maximum Length	Description
Template Name *	50	Specify a name for your template to uniquely identify it from other existing templates.
Displayed Title *	50	Specify a subject to display with the message.
Choose a Template Category:	n/a	Select one of the following categories for your template: • **Staff Event** — Messages specific to staff members. For example, a staff meeting event notification to specific group members or a staff meeting invite to staff members. • **Patient Event** — Messages specific to an event related to a patient. For example, notifications for the care team members when a patient requests counseling, or notifications to request a visit from the chaplain. • **Location Event** — Messages specific to events happening at a location. For example, room security or room clean-up requests. • **Mass Notification** — Messages for more than 50 recipients. For example, urgent notifications on a security breach and lock down, or severe weather alerts and warning. If you do not specify a category, the Staff Event category is selected by default.
Facility*:	50	Select a facility from the dropdown list. If you have not defined a facility, or if you do not want to specify a facility for the new template, select the default **Global** value

3. In the Recipient Options section, complete the fields listed in the table below.

Field	Description
Choose a Template Recipient	Select one of the following recipient types: • **My Department** — Select if your template recipients are members of "My Department." • **Custom** — Select if your template recipient delivery mechanism is based on the clinical workflow engine's rules. Using the **Custom** field requires custom configuration. When the Custom field is selected, **Time to Live** and **Response Timeout**, options are hidden in the **Delivery Options** section. • **Care Team** — Select if your template recipients are members of your care team. Care team includes all the people who are assigned to take care of a patient. • **Care Team Member** —Select if your template recipient is an individual Care Team member. **Note:** The **Care Team** and **Care Team Member** options are displayed only when you select the **Patient Event** or **Location Event** categories in the **Choose a Template Category:** field. • **Group** — Select to choose a specific group from the **Find a Group** pop up list as your template recipient. • **Selected Group** — Select to choose a range of groups between 2 to 100 as your template recipients. **Note:** If you selected **Group** or **Selected Group** options, then you must enter a response for these selections.
Recipient Label *	Recipient Label is auto-populated when you choose any template recipient option, except the Group option.

4. Specify one of the following Response Options types:
   - **Accept/Decline** — Select this option to receive an Accept or Decline notification from the recipients.

- **Multiple Choice Response** — Select this option to allow the recipients to respond with multiple types of custom responses.
  - Select the **New Response** field to enter a text for the response, and select the plus sign to add this response as a choice. You can continue to add more responses, as shown in the following screenshot.



  - If you select this option, you must enter at least one response. The maximum number of responses is limited to 20.
  - You cannot enter responses that are blank, duplicate, or more than 50 characters long.
- **None** — Select this option if no response is needed from the recipients.

Note: The Response Options are not available if you chose a **Mass Notification** template category.

5. Specify the following information in the Information Section Content section:
   - **Displayed Information** — Enter a text up to 500 characters to display as the template information. This field is required as a default when the **Sender can edit this** field is selected.
   - **Sender can edit this** — Select this checkbox to allow the sender to edit the message. This checkbox is disabled by default.
   - **Form Label** — Enter a new label in the **Form Label** field. User can use the labels as a guide to initiate a conversation and provide some specific information. For example, for a Staff Meeting template, you can configure 3 labels such as Time, Place, and Location. Users initiating the Staff Meeting template will see 3 text areas with the label for which they are required to enter a response. The maximum number of the Form Labels supported is 20. You cannot have Form labels that:
     - Have the ^ character.
     - Are blank or duplicate.
     - Are more than 50 characters long.
6. Specify the **Delivery Options** section.

Field	Maximum Length	Description
Priority	n/a	Specify a priority. You can choose one of the following priority types: • **Normal** • **High** • **Urgent**
Time to Live * (Minutes)	99999 minutes	Specify the duration for which the event message is displayed on the recipient's device. Enter Time to Live value in minutes. Default is 10 minutes. The maximum response time value that you can enter is limited to 99999 minutes. **Note:** You cannot enter a negative value for this field.

Field	Maximum Length	Description
Response Timeout (Seconds)	999999 seconds	Specify a time for the response time limit. Enter a Response Timeout value until when the recipients can respond to a message or event notification. Default response time value is 5 minutes. The maximum response time value that you can enter is limited to 999999 seconds, and the minimum response time value is limited to 10 seconds. **Note:** This field is not available for **Mass Notification** templates and when Response Option is set to **none**.
Confirmation Message	500	Enter a confirmation message.
Exclude Sender	n/a	Choose **Yes** or **No** to exclude or include the person initiating the template as a recipient. The default value is **No**. As an initiator of the template, you may want to receive the notifications for certain events and a default **No** value allows you the receive the notifications. In some situations, when you do not want to receive any notifications, you can set the value for **Exclude Sender** field to **Yes**. For example, if you are triggering a room cleanup template, you may not want to receive any notifications regarding this event. You can choose **Yes** to exclude yourself from receiving notification **Note:** This field is not available for Mass Notification templates.

7. In the Sharing Options section, click **Add Group** to display the Find a Group dialog box.
   Use the Find a Group dialog box to:
   - Enter the group name in the Group Name field to search for a group in the system.
   - Select multiple groups from the list.
   - Toggle the **Facility Name** field to view all facilities available in your system and refine your search.

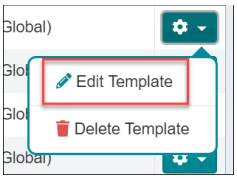
   Note: All members of the groups added under Sharing Options can view the templates on their devices.
8. Click **Find Group** in the **Administrative Group** field to display the Find a Group dialog box.
   Select a Group with members who can send messages and complete alerts, such as a Mass Notification alert.
   1. In the **Group Name** field, enter the name of the group that you want to share the templates with.
   2. Click **Select Group** to close the Find a Group dialog box.
9. Select one of the following to close the New Template page.
   - **Save** — to add the new template to the system.
   - **Cancel** — to return to the **Templates** page without adding a template.

Editing a Template

You can edit the information for an existing template in the Vocera Platform Web Console

1. Click **Templates** in the **Manage** section to display a list of available Templates.
2. Locate the Template that you want to edit.
3. Click the **Options** button in the far right of this template.

4. Select **Edit Template** from the dropdown menu in the **Options** button.



The Edit Template page displays

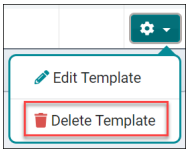
You can also click on the template that you want to edit and the Edit Template page displays.

5. Edit the template information as necessary. See Adding a Template on page 249 for a list of the template fields.
6. Select one of the following to close the Edit Template page.
   - **Save** — to update the template and save changes to the system.
   - **Cancel** — to return back to the **Templates** page without adding a template.

Deleting a Template

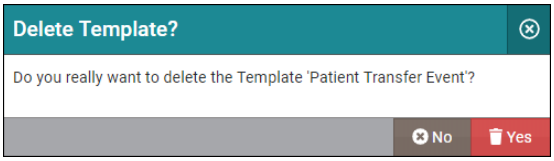
You can delete an existing template in Vocera Platform Web Console.

1. Navigate to **Templates** from the **Manage** section and locate the template that you want to delete.
2. Choose one of the following:
   - Click on the template that you want to delete, and select **Delete Template** button on the top left corner of the Edit Template page.
   - Click the **Options** button in the far right of the template, and select **Delete Template** from the dropdown menu.



The system displays a confirmation message to confirm if you really want to delete the selected template.

For example, if you selected **Delete Template** for a Patient Transfer Event template, the following confirmation message appears on the screen:



3. Select one of the following to close the Delete Template dialog.
   - **Yes** — to complete the delete action.
   - **No** — to cancel the delete action.

Bulk Actions

Quickly perform bulk activities, such as importing or exporting bulk data to the system.

You can use the **Bulk Actions** in the Vocera Platform Web Console to enter a large amount of the same kind of data at a single time using 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 creating each user individually in the Web Console

You may occasionally want to export large sets of data from the Vocera database to a CSV file, you can also perform a bulk export activity through **Bulk Actions** in the Web Console.

Importing Data

A CSV file lets you specify most of the information you can enter when you create an entry in the Web 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 of the **Add New User** dialog box.

Exporting Data

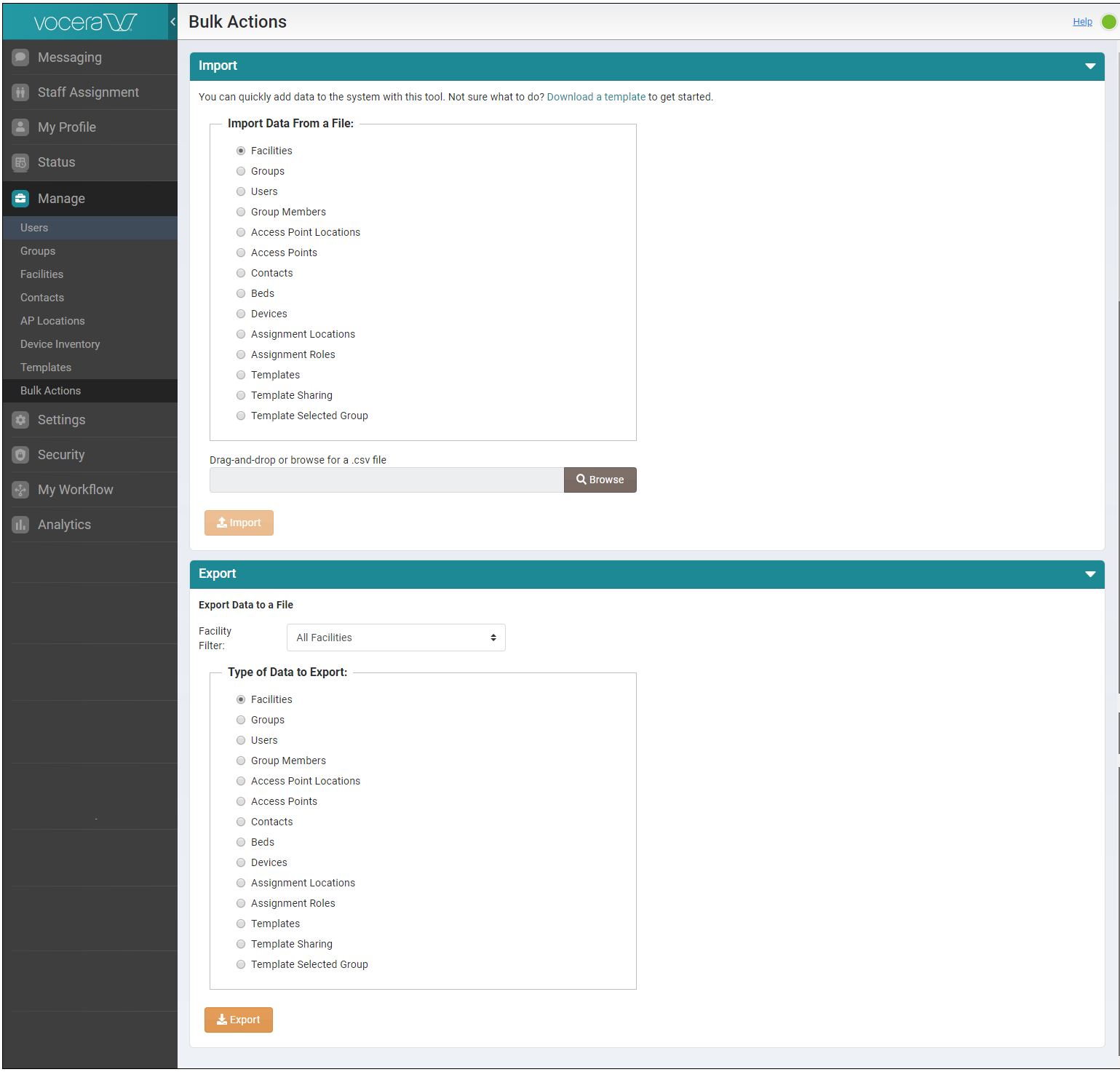
Exporting data is useful when you want to examine all your data or make global changes that might be time consuming if you were to make these changes in the Web Console.

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.

Note:

- Exporting data does not remove the data from the database.
- Vocera supports numeric values in name fields. The Web Console lets you create a purely numeric name that begins with a zero, such as `012345`

To import and export from the Vocera Platform Web Console, select **Bulk Actions** in the **Manage** section of the navigation bar.



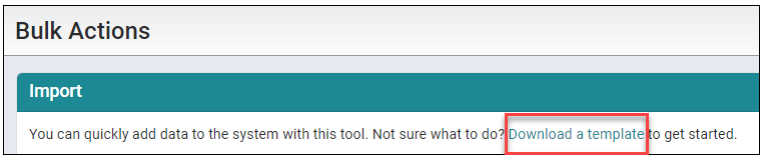
Note: There is a current known issue that will allow an upload of a concatenated Personal and Business contact. Please ensure that there is one set of information per line in the CSV file.

Importing Data to the System

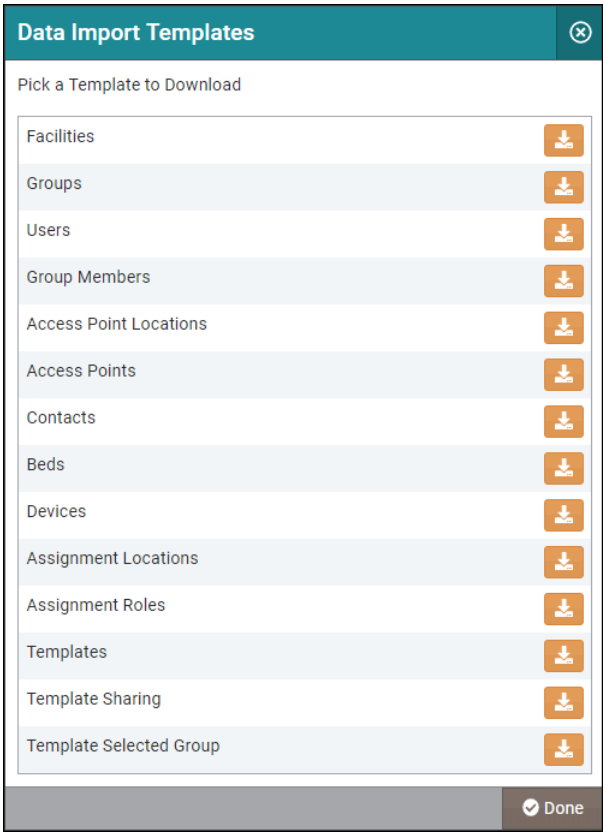
Quickly upload bulk data to the system using pre-defined templates and import bulk data to the system.

1. Select **Bulk Actions** in the **Manage** section.
   The Bulk Actions page displays.

2. In the Import section, click on **Download a template**.
   The data import templates are in Microsoft Excel format. Use these templates to enter the data you want to load, then save them in CSV format.



   A pop-up displays with a list of available data import templates.

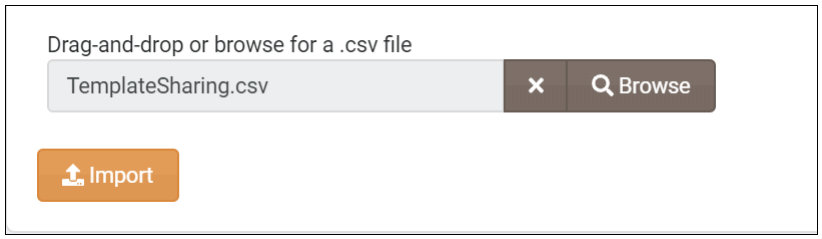


3. Select the template that you want from the Data Import Templates list.
   You can use choose one of the following template types:

Type of Data	Template
Facilities	`Facilities-template.CSV`
Groups	`Groups-template.CSV`
Users	`Users-template.CSV`
Group Members	`GroupMembers-template.CSV`
Access Point Locations	`AccessPointLocations-template.CSV`
Access Points	`AccessPoints-template.CSV`
Contacts	`Contact-template.CSV`
Beds	`Beds-template.CSV`
Devices	`Devices-template.CSV`
Assignment Locations	`AssignmentLocations-template.CSV`

Type of Data	Template
Assignment Roles	`AssignmentRoles.CSV`
Templates	`Templates-templates.CSV`
Template Sharing	`TemplateSharing.CSV`
Template Selected Group	`TemplateSelectedGroup-template.CSV`

4. Click on the download icon next to the template that you want to download.
   The selected data import template Microsoft Excel CSV file is downloaded to the download folder on your computer.
5. Open the downloaded CSV file in a supported application (for example, Microsoft Excel) and update the information.
6. Click **Browse** to locate your updated CSV file on your computer and upload it to the system. You can also drag and drop the file from your desktop.
   The following screenshot shows a TemplateSharing.CSV file uploaded from a computer.

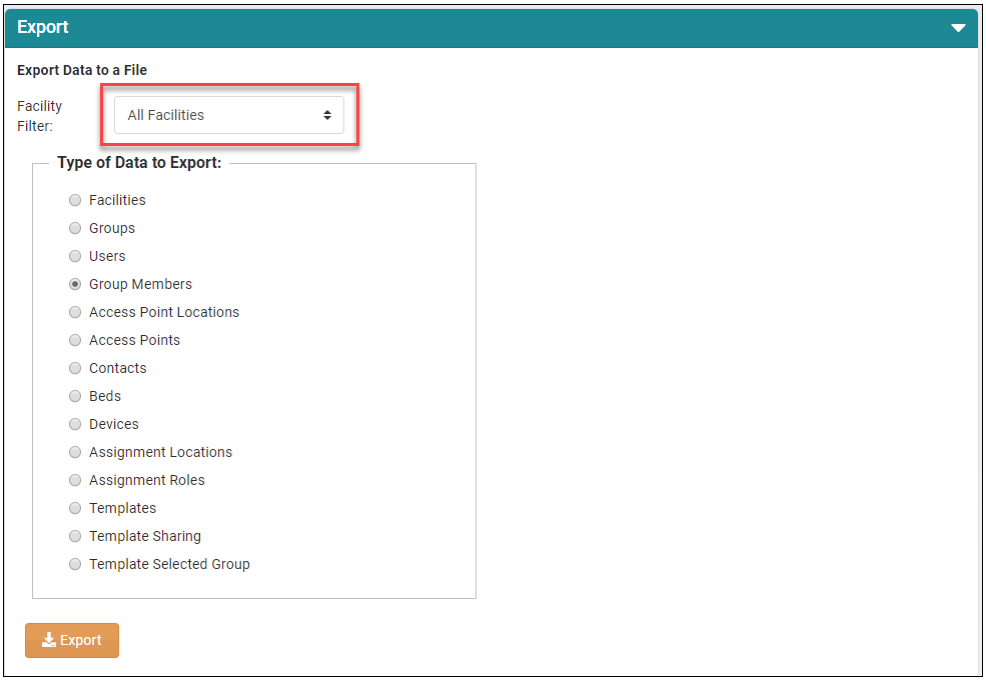


   The **Import** button activates only after you drag and drop or upload a CSV file in the Browse field.
7. Click **Import** to import the uploaded CSV file to the system.
   The system validates the imported file and displays a Validation Result with the information on the fields processed through the import action.

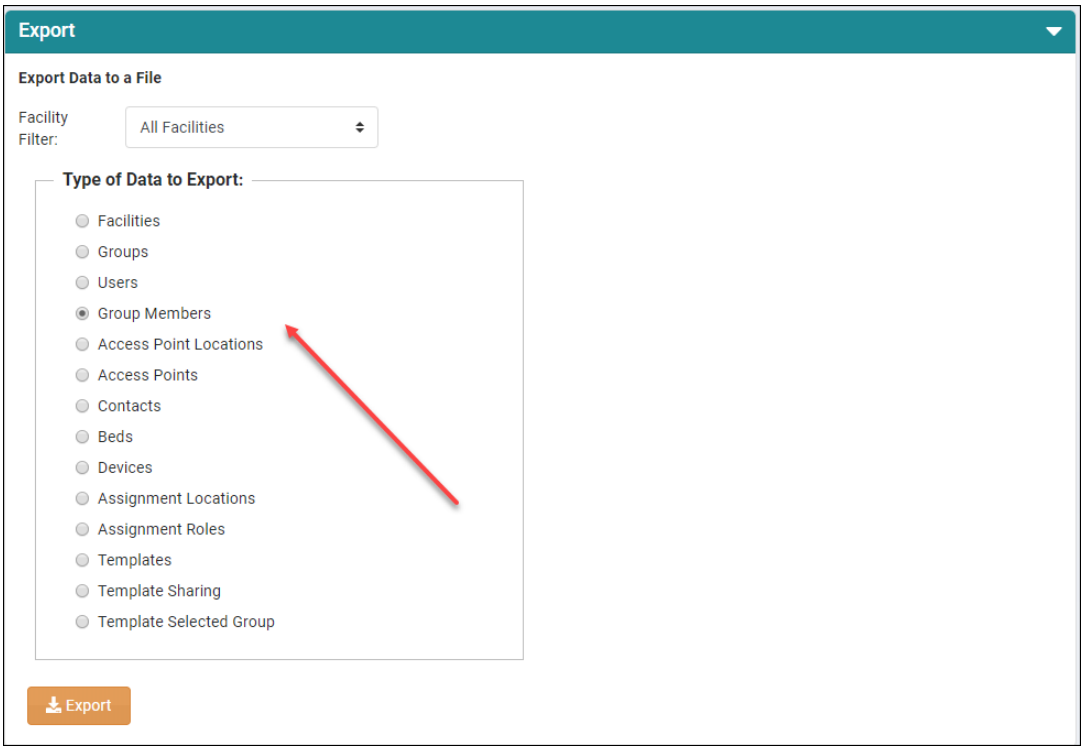
Exporting Data to a CSV File

Export data in your Vocera system to your computer in a CSV file format.

1. Select **Bulk Actions** in the **Manage** section.
   The Bulk Actions page displays.
2. Scroll down to the Export configuration section and click on the Facility Filter dropdown to choose a facility for which you want to export the data.



3. Click on a radio button to choose a type of data that you want to export from the **Type of Date to Export** list.



4. Click the **Export** button to download a CSV file with the selected data type on your computer.

   The selected data type is downloaded to the download folder on your computer in a Microsoft Excel CSV file format.

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.

Template Reference

Review the list of template available in the Bulk Actions page of the Web Console

The Facilities Template

The Facilities template (`facilities-template.CSV`) lets you create Vocera facilities in bulk.

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

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Facility Name	50	Enter the name of the facility in the **Facility 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 facilities. If users refer to a facility 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 facility that has a Vocera SIP Telephony Gateway associated with it, you must set the value of the VOCERA_FACILITY environment variable on the telephony server machine to the name of the new facility.
Alternate Spoken Facility Name	50	Enter the **Alternate Spoken Facility Name** to enable Vocera to recognize variations of the exact facility name. For example, if users commonly refer to a facility by a nickname or an acronym, enter that variation here.

Field	Maximum Length	Description
Description	100	Enter a description of the facility in the **Description** field.
Cost Center	100	Enter the **Cost Center** to specify a cost center for the facility.
Time Zone	n/a	The **Time Zone** specifies a time zone for the facility. By default, a facility's time zone is the Vocera Platform time zone.
Emergency Broadcast Group	n/a	Enter the **Emergency Broadcast Group** name to specify the name of the group that receives emergency broadcasts for this facility. If you set up an emergency broadcast group, a user can initiate an urgent broadcast by clicking the Call button twice. Everyone in the group hears the caller immediately—no speech recognition or Genie interactions are necessary.
Emergency Broadcast Group Facility	n/a	Specifies the name of the Facility for the Emergency Broadcast Group.
Initiate Emergency Broadcast Silently	n/a	Specifies whether to initiate emergency broadcasts at this facility silently, without playing a chime first. This option is available only if a group is specified in the **Emergency Broadcast Group** field. By default, it is unchecked.

The Groups Template

The Groups template (`groups-template.CSV`) lets you create Vocera groups.

If you specify a facility, it must already exist in the database; the template does not create it. If a row in this data-loading template references a facility that does not exist, the row causes a validation error and does not load. All other rows that successfully validate are loaded properly.

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 import file.

The following table describes the fields names, maximum length for fields names, and a brief description of the 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 Name**.
Facility	50	Use the **Facility** field to specify the group's home facility. If your organization has multiple facilities connected to the same Vocera server, choose the home facility that represents the member's physical location. If the group's membership spans multiple facilities, specify **Global**. The **Facility** field is treated differently if you are importing or updating groups: • When importing groups, you can leave this field blank to specify the **Global** facility. • When updating groups, the **Facility** field is required. You cannot leave the field blank.

Field	Maximum Length	Description
Alternate Spoken Name	50	In the **Alternate Spoken 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."
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.
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 all** sales people."
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.
Forwarding Type		Specify one of the Standard Options: None, Contact, Off Network Group Member, Phone, Pager. **Note:** You must configure a pager number to use Pager as a standard option. If the Forwarding field references a user or contacts entry that does not exist in the Vocera database, the record will be skipped when you try to import it. To avoid data validation errors, Vocera recommends importing group data in multiple passes.

Field	Maximum Length	Description
Forwarding To - Type		Specify one of the Standard Options: Groups, Users, Business Contacts, Personal Contacts - Required if Forwarding Type Set to contact. The following options are used to differentiate contact types Groups, Users, PersonalContacts, BusinessContacts **Note:** You must enter a value for **Personal Contacts** if **Forwarding Type** is set to **Contact**. The following options are used to differentiate contact types: Groups, Users, Personal Contacts, and Business Contacts.
Forwarding To - Group or Business Contact Name	50	Specify a Group Name that starts with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). Specify a Business Contact Name that starts with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). **Note:** The Business Contact Name or Group Name is required if the **Forwarding To - Type** is set to **Groups** or **Business Contacts**.
Forwarding To - User or Personal Contact First Name	50	User First Name - Specify a user's first name, name must start with a letter or digit. User's first name must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). **Note:** User's first name is required if the **Forwarding Type** is **Contact** and **Forwarding To Type** is **User**. Personal Contact First Name - Specify a first name for a personal contact, name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). **Note:** Personal Contact first name is required if the **Forwarding To Type** is set to **Users** or **Personal Contacts**.
Forwarding To - User or Personal Contact Last Name	50	User Last Name - Specify a user's last name, name must start with a letter or digit. User's last name must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). **Note:** User Last Name is required if the **Forwarding Type** is **Contact** and **Forwarding To Type** is **User**. Personal Contact Last Name - Specify a last name for a personal contact, name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). **Note:** Personal Contact last name is required if the **Forwarding To Type** is set to **Users** or **Personal Contacts**.
Forwarding To - User Login	50	Specify a user name that starts with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), periods (.), underscores (_), or dashes (-). **Note:** This field information is required if the **Forwarding Type** is a **Contact** and **Forwarding To Type** is **Users**.

Field	Maximum Length	Description
Forwarding To - User, Group, or Contact (Facility)	50	Specify an entry for a particular user, group, or contact entry when no members of the original group can take the call. This ensures the calls are transferred to the field information entered. The user, group, or contact entry name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). This field information depends on **Forwarding To - Type of Personal Contacts, Business Contacts, Users, Groups** field.
Forwarding To - Another Number	100	Specify the phone number to forward the calls. This field information must be provided if forwarding type of phone is set..
Emergency Broadcast Group	50	Specify the name of the group that receives emergency broadcasts for a functional group. Group name that starts with a letter or digit. Name must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-).
Emergency Broadcast Group (Facility)	50	Specify a facility name that starts with a letter or digit. Name must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). This field information depends on the **Emergency Broadcast Group** being set.
Group Type	n/a	Specify either **Department**, **Subdepartment**, or **Ordinary** (the default). • **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. • **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. If you provide a value other than **Department**, **Subdepartment**, or **Ordinary** in the data-loading template, an error will occur when you try to import the file. If you specify **Department**, the **PIN for Long Distance Calls** and **Cost Center** fields can also be entered for accounting purposes.
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.

Field	Maximum Length	Description
Forwarding 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.
Remove Users on Logout	n/a	Specify either **True** or **False** (the default) to indicate whether membership in the group is temporary. If you enter **True**, 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 facility 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.
Pager Number	75	Specify the pager number for the group. 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.
Off-Site Calls	n/a	Specify either **True** or **False** to indicate whether calls to the group can be received by members who are currently at a different facility from the caller. If your Vocera system has only one facility, this option does not apply. If you don't want members of the group to receive calls from people at other facilities, specify **False**.
Off-Site Broadcasts	n/a	Specify either **True** or **False** to indicate whether broadcasts to the group can be received by members who are currently at a different facility from the person who initiated the broadcast. If your Vocera system has only one facility, this option does not apply. If you don't want members of the group to receive broadcasts from people at other facilities, specify **False**.
Manager Group	50	Specify the group whose members can manage the group you are importing. To qualify a group by specifying its facility, use a colon to separate the value from the facility name (GroupName:FacilityName). If you do not specify a facility, the facility of the group you are importing is used by default.
Manager Group Facility	50	Specify a facility name that starts with a letter or digit. Name must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). This field information depends on the **Manager Group** \ being set.

Field	Maximum Length	Description
Add Group	50	Specify the group whose members are allowed to add themselves to the group you are importing. To qualify a group by specifying its facility, use a colon to separate the value from the facility name (GroupName:FacilityName). If you do not specify a facility, the facility of the group you are importing is used by default.
Add Group Facility	50	Specify a facility's name, facility name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). This field information depends on the **Add Group** being set.
Device Group	50	Specify the group's name whose members manage the Vocera devices used by the group you are importing.
Device Group Facility	50	Specify a facility name that starts with a letter or digit. Name must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-). This field information depends on the **Device Group** being set.
Permission Only	n/a	Specify either **True** or **False** to indicate whether the group is used to grant or revoke permissions only and should not be callable. If you specify **True**, calling and broadcasting to this group will be disabled.
Forward on Broadcast Number	n/a	Specify to forward a call to a broadcast number, there is no character limit for this field.
Forward on Conference Number	n/a	Specify to forward a call to a Conference call, there is no character limits for this field.
Voice Mail Enabled	n/a	Specify either **True** or **False** to indicate whether the voice mail is enabled or not.

The Users Template

The Users template (`Users-template.CSV`) lets you create new users.

If you specify a facility, department, or conference group, it must already exist in the database; the template does not create it. If a row in this data-loading template references one of those entities, and that entity does not exist, the row causes a validation error and does not load. Any other rows that successfully validate load properly.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
User Login	50	Enter a **User Login** 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 Login**.
Last Name	50	Enter the user's **Last Name** and **First 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.
First Name	50	Enter the user's **First 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.
Facility		Specify the name of the facility for the use. If you have not defined any facility, or if you do not want to specify a facility for the new user, use the default Global value for this group.
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.
Email	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 integrate the user with Vocera Messaging Platform (VMP). If so, enter a unique email address. Otherwise, the VMP 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.

Field	Maximum Length	Description
Desk Phone or Extension	75	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	75	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	75	Allows users to forward calls from their badges to their home phones. It also allows users take advantage of the "Call My House" entry in Contacts.
Alternate Spoken Name 1, Alternate Spoken Name 2, Alternate Spoken Name 3	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. • 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 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`. When you import or update Vocera users using a CSV file, the Alternate Spoken Name values are treated as a set. A user's Alternate Spoken Name fields are replaced by any Alternate Spoken Name values in a CSV row. If all three Alternate Spoken Name fields in a CSV row are empty, no changes will be made to those fields when you update the user. To remove all alternate spoken names for a user, enter the literal string value `*blank*` in all three Alternate Spoken Name fields in a CSV row.
Device ID	12	Enter the MAC address of the user's badge in the **Device 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 Vocera device 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.

Field	Maximum Length	Description
Home Department	50	Specifies the user's home department. When you import users through the data-loading template, any value in this field is also imported. When you export users to a `.csv` file, Vocera populates this field for informational purposes.
Home Department Facility	50	Specifies the facility for the user's home department.
Conference Group	n/a	Optionally assign the user to a conference group by specifying it here. The template does not create a conference group, it must already exist in the database. If the group does not exist, the row results in a validation error and fails to load. To qualify a conference group by specifying its facility, use a colon to separate the value from the facility name (GroupName:FacilityName). If you do not specify a facility, the value of the **Facility** field is used by default.
Conference Group Facility		
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**.
Cost Center		
PIN for Long Distance Calls	75	Allows an organization to authorize or account for telephone usage and to distribute telephone costs among different users, departments, or facilities. A PIN template can include digits, special characters, and PIN macros.
Expiation Date	10	Enter the last full day that a temporary user account is available. The date string must be specified using the following date format: United States and Canada: `mm/dd/yyyy` Other locales: `dd/mm/yyyy` For example, the fourth day of September in the year 2010 is written as 09/04/2010 in mm/dd/yyyy format and 04/09/2010 in dd/mm/yyyy format.

The Group Members Template

The Group Members template (`GroupMembers-template.CSV`) lets you add Vocera users to groups.

All the users and the groups must already exist in the database; the template does not create them. If a row in this data-loading template references one of those entities, and that entity does not exist, the row causes a validation error and does not load. Any other rows that successfully validate load properly.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Group Name	50	Enter a group name starting with a letter or digit. Group names can contain letters, digits, spaces,apostrophes ('), underscores (_), or dashes (-).
Group Facility	50	Enter the name of the facility to which this group belongs. Facility names can contain letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-).

Field	Maximum Length	Description
Member Name (User)	50	Enter the username (member for this group). User's name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), periods (.), underscores (_), or dashes (-).
Member Name (Group)	50	Name must start with a letter or digit. It must contain only letters, digits, spaces, apostrophes ('), underscores (_), or dashes (-).
Member Facility (Group)	50	Enter the name of the Facility to which this group belongs.

The Access Point Locations Template

The Access Points Locations template (`AccessPointLocations-template.csv`) lets you associate the name of a Vocera facility with each of your access points.

All the locations must already exist in the database; the template does not create them. If a row in this data-loading template references an access point that does not exist, the row causes a validation error and does not load. Any other rows that successfully validate load properly.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Location Name	50	Enter the name of the AP Location that already exists.
Alternate Spoken Location Name	50	Enter and alternate name for the location. For example, if users commonly refer to a facility by a nickname or an acronym, enter that variation here.
Description	100	Enter a description of the facility.
Facility	50	Enter the name of the facility for this AP location. 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 facilities. If users refer to a facility 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 facility that has a Vocera SIP Telephony Gateway associated with it, you must set the value of the VOCERA_FACILITY environment variable on the telephony server machine to the name of the new facility.

The Access Points Template

The Access Points template (`AccessPoints-template.csv`) lets you create associate the name of a Vocera facility with the MAC address of your access points.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Location Name	50	Enter the name of a location that already exists. To qualify a location by specifying its facility, use a colon to separate the value from the facility name (LocationName:FacilityName). If you do not specify a facility name, the Global facility is used by default.

Field	Maximum Length	Description
Mac Address	12	Enter the MAC address (12 hexadecimal characters) of the access point that you want to assign to this location. 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.
Facility	50	Enter the name of the facility in for this access point. 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 facilities. If users refer to a facility 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 facility that has a Vocera SIP Telephony Gateway associated with it, you must set the value of the VOCERA_FACILITY environment variable on the telephony server machine to the name of the new facility.

The Contacts Template

The Contacts template (`Contacts-template.csv`) lets you create contacts and add the basic information for contacts.

When you add a contact to your system you provide basic information to identify the entry, and contact information such as phone numbers and email addresses.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Place Name	50	If the new contact is a place, specify the name of the place.
Last Name	50	If the new contact is a person, specify the last name of the contact.
First Name	50	If the new contact is a person, specify the first name of the contact.
Identifying Phrase	100	Specify an Identifying Phrase to help Vocera distinguish this contact from another whose first and last names are spelled the same.
Email Address	60	Specify an email address for the contact.
Phone	n/a	Specify the phone number for the new contact.

Field	Maximum Length	Description
Alternate Spoken Name 1	50	Enter the Alternate Spoken Name 1. Use these guidelines to ensure the best result when you are defining alternate names for users: • **Person, Group, and Location Names**–If users refer to a person, group, or location 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. • **Digits in Name Fields**–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 these special characters are allowed, it is unlikely that an alternate spoken name would need underscores (_), or dashes (-). • **Staff IDs**–It is recommended that you do not create an alternate spoken name that contains numeric digits only. For example, a staff ID with numbers and no letters. `567748` Entering numeric staff IDs is permitted. However, using numeric values only might result in • Slower Genie response times • Problems with phone number recognition • **Acronyms and Initials in Alternate Spoken Names**–If people use an acronym or initials to refer to an entry in Contacts, 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. For Armandeep Munindar Gill, also enter A M Gill rather than A.M. Gill. • **Unusual Pronunciation**–If a name has an unusual or confusing pronunciation, or silent letters, 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. • **Professional Titles in Alternate Spoken Names**–If users refer to a person by his or her title, provide the full spelling of the title rather than an abbreviation. For example, enter Father Brown instead of Fr. Brown, or Professor Lindsay instead of Prof. Lindsay.

Field	Maximum Length	Description
Alternate Spoken Name 2	50	Enter the Alternate Spoken Name 2. Use these guidelines to ensure the best result when you are defining alternate names for users: • **Person, Group, and Location Names**–If users refer to a person, group, or location 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. • **Digits in Name Fields**–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 these special characters are allowed, it is unlikely that an alternate spoken name would need underscores (_), or dashes (-). • **Staff IDs**–It is recommended that you do not create an alternate spoken name that contains numeric digits only. For example, a staff ID with numbers and no letters. `567748` Entering numeric staff IDs is permitted. However, using numeric values only might result in • Slower Genie response times • Problems with phone number recognition • **Acronyms and Initials in Alternate Spoken Names**–If people use an acronym or initials to refer to an entry in Contacts, 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. For Armandeep Munindar Gill, also enter A M Gill rather than A.M. Gill. • **Unusual Pronunciation**–If a name has an unusual or confusing pronunciation, or silent letters, 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. • **Professional Titles in Alternate Spoken Names**–If users refer to a person by his or her title, provide the full spelling of the title rather than an abbreviation. For example, enter Father Brown instead of Fr. Brown, or Professor Lindsay instead of Prof. Lindsay.

Field	Maximum Length	Description
Alternate Spoken Name 3		Enter the Alternate Spoken Name 3. Use these guidelines to ensure the best result when you are defining alternate names for users: • **Person, Group, and Location Names**–If users refer to a person, group, or location 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. • **Digits in Name Fields**–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 these special characters are allowed, it is unlikely that an alternate spoken name would need underscores (_), or dashes (-). • **Staff IDs**–It is recommended that you do not create an alternate spoken name that contains numeric digits only. For example, a staff ID with numbers and no letters. `567748` Entering numeric staff IDs is permitted. However, using numeric values only might result in • Slower Genie response times • Problems with phone number recognition • **Acronyms and Initials in Alternate Spoken Names**–If people use an acronym or initials to refer to an entry in Contacts, 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. For Armandeep Munindar Gill, also enter A M Gill rather than A.M. Gill. • **Unusual Pronunciation**–If a name has an unusual or confusing pronunciation, or silent letters, 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. • **Professional Titles in Alternate Spoken Names**–If users refer to a person by his or her title, provide the full spelling of the title rather than an abbreviation. For example, enter Father Brown instead of Fr. Brown, or Professor Lindsay instead of Prof. Lindsay.
Pager Phone	50	Provide a pager number for the person or place in the **Pager** field.

The Beds Template

The Beds template (`Beds-template.csv`) lets you create and upload data on beds and related information.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Bed	100	Specifies the name or number of the bed.
Pillow Number	50	Specifies the pillow number to access the bedside phone.
Room	n/a	Specifies the number of a room associated with the bed.
Room Name	100	Specifies the name or number of room associated with the bed.

Field	Maximum Length	Description
Unit	n/a	Specifies the name or number of unit associated with the bed A unit is a hospital unit, such as Dialysis, Cardiac Intensive Care, or Surgical Oncology, which has beds with nurses assigned to them. These units must be defined in the Staff Assignment application.
Facility	100	Specifies the name of the facility associated with room 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.

The Devices Template

The Devices template (`Devices-template.xls`) lets you add or update Vocera devices.

If you specify a facility, group, or device status, it must already exist in the database; the template does not create it. If a row in this data-loading template references one of those entities, and that entity does not exist, the row causes a validation error and does not load. All other rows that successfully validate will load properly.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
MAC Address	12	Specifies the Media Access Control address (MAC address) is a hardware address that acts like a unique name for the device. The MAC address is 12 characters long. Most MAC addresses for Vocera badges have the following prefix: `0009ef`. Adding devices • For B3000 badges, this field is optional because the MAC address can be derived from the serial number; the last 6 characters of the MAC address and the serial number are identical. • For Smartphones, this field is required. Updating devices • The MAC Address field is required for all device types as it is the key field that uniquely identifies devices in the database.
Serial Number	15	Specifies the serial number of the Vocera device. For most Vocera badges, the serial number is 12 characters. For V5000 Smartbadge the serial number is 14 characters. For Vocera Smartphones, the serial number is 10 characters.
Device Type		Specifies the type of the Vocera device. **Note:** The **Device Type** field column is calculated and included in the import CSV file if the **Serial Number** of the device is filled in.
Color	n/a	Specifies the color of your Vocera device. **Note:** The **Color** field column is calculated and included in the import CSV file if the **Serial Number** of the device is filled in.
Label	20	Specifies a label that uniquely identifies the device.

Field	Maximum Length	Description
Status	n/a	Specifies the status of devices.
Tracking Date	n/a	Specifies a date to track the device. For example, you can track when the device was sent for repair or return merchandise authorization (RMA).
Owning Group	n/a	Specifies the group that owns a device.
Owning Group Facility	n/a	Specifies the facility that owns a device.
Notes	1000	Specifies a multi-line text box that lets you provide further information about the device status. For example, "Device stopped working on [DATE] after accidentally being immersed in water" or "Device sent to IT to repair the battery latch."
Facility	n/a	Specifies the device's home facility.
Shared ?	n/a	Specifies whether the device is shared by multiple group members.
Disabled ?	n/a	Specifies if the device is disabled.

The Assignment Locations Template

The Assignment Locations template (`AssignmentLocations-template.CSV`) lets you associate a location for the assignments.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Location ID	n/a	Specifies the attribute that stores the unique identifier for the location.
Location Name	50	Specifies the attribute that stores the name of the location.
Location Order	n/a	Specifies the order the location to be displayed in the staff assignment client.
Location Facility	50	Enter the name of the Facility associated with this location.
Bed	100	Specifies the name or number of Beds associated with this location.
Room	100	Specifies the name or number of Rooms associated with this location.
Department	50	Specifies the name of the Departments associated with this location.
Bed Facility	n/a	Specify the name of the facility associated with bed.

The Assignment Roles Template

The Assignment Roles template (`AssignmentRoles-template.CSV`) lets you add role assignments.

If a row in this data-loading template references one of those entities, and that entity does not exist, the row causes a validation error and does not load. Any other rows that successfully validate load properly.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Name	50	Enter the name of a functional role for staff assignment. For example, Charge Nurse is a functional role.
Abbreviation	n/a	Enter an abbreviation used for the assignment role. For example, CN could be an abbreviation for Charge Nurse.
Facility	50	Enter the name of the Facility for thie assignment role. 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.
Order	n/a	Specifies ordinal number for sorting roles.
Active Flag	n/a	Indicates if active, specify True or False to indicate if active.

The Templates Template

The Group Members template (`groupmembers-template.CSV`) lets you add the Vocera templates for alerts and critical messages.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Template Name	50	Enter a name for your template to uniquely identify it from other existing templates.
Displayed Title	50	Enter a subject to display with the message.
Template Category	n/a	Enter one of the following categories for your template: • Staff Event — Messages specific to staff members. For example, a staff meeting event notification to specific group members or a staff meeting invite to staff members. • Patient Event — Messages specific to an event related to a patient. For example, notifications for the care team members when a patient requests counseling, or notifications to request a visit from the chaplain. • Location Event — Messages specific to events happening at a location. For example, room security or room clean-up requests. • Mass Notification — Messages for more than 50 recipients. For example, urgent notifications on a security breach and lock down, or severe weather alerts and warning. If you do not specify a category, the Staff Event category is selected by default.
Facility	50	Enter the name of the facility in the **Facility 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.
Recipient Type	n/a	Enter one of the following recipient types: • My Department — Select if your template recipients are members of "My Department." • Custom — Select if your template recipient delivery mechanism is based on the clinical workflow engine's rules. Using the Custom field requires custom configuration. When the Custom field is selected, Time to Live and Response Timeout, options are hidden in the Delivery Options section. • Care Team — Select if your template recipients are members of your care team. Care team includes all the people who are assigned to take care of a patient. • Care Team Member —Select if your template recipient is an individual Care Team member. **Note:** The Care Team and Care Team Member options are displayed only when you select the Patient Event or Location Event categories in the Choose a Template Category: field. • Group — Select to choose a specific group from the Find a Group pop up list as your template recipient. • Selected Group — Select to choose a range of groups between 2 to 100 as your template recipients. **Note:** If you selected Group or Selected Group options, then you must enter a response for these selections.
Recipient Group	n/a	Enter the name of the group that is the recipient of the template.
Recipient Group Facility	50	Enter the facility associated with the recipient group facility.

Field	Maximum Length	Description
Recipient Label	n/a	Recipient Label is auto-populated when a template recipient option is chosen. The Group recipient option is an exception to this field.
Displayed Information	500	Enter a text that displays as part of the template information.
Sender Editing	n/a	Specifies that sender can edit the message when the **Sender can edit this** checkbox is enabled.
Form Label	50	Allows user to enter a new label in the Form Label field. User can use the labels as a guide to initiate a conversation and provide some specific information. For example, for a Staff Meeting template, you can configure 3 labels such as Time, Place, and Location. Users initiating the Staff Meeting template will see 3 text areas with the label for which they are required to enter a response. The maximum number of the Form Labels supported is 20.
Priority	n/a	Allows to choose one of the following priority types: • Normal • High • Urgent
Time to Live	99999 minutes	Enter the duration for which the event message is displayed on the recipient's device. Enter Time to Live value in minutes. Default is 10 minutes. The maximum response time value that you can enter is limited to 99999 minutes. **Note:** You cannot enter a negative value for this field.
Confirmation Message	500	Enter a confirmation message.
Response Timeout	n/a	Specify a timeout value for sending responses.
Exclude Sender	n/a	Specify to exclude or include the person initiating the template from receiving the template alert. Choose a Yes or No value.
Administrator Group	50	Specify Administrator Group name.
Administrator Group Facility	50	Specify name of the Facility associated with the Administrator Group.
Response Type	n/a	Enter one of the following response types: • **Accept/Decline** — Select this option to receive an Accept or Decline notification from the recipients. • **Multiple Choice Response** — Select this option to allow the recipients to respond with multiple types of custom responses. Select the New Response field to enter a text for the response, and select the plus sign to add this response as a choice. You can continue to add more responses, as shown in the following screenshot. If you select this option, you must enter at least one response. The maximum number of responses is limited to 20. You cannot enter responses that are blank, duplicate, or more than 50 characters long. • **None** — Select this option if no response is needed from the recipients.

Field	Maximum Length	Description
Multiple Choice Response 1 through 20	n/a	Allows to upload up to 20 types of multiple choice responses when Multiple Choice response type is selected. **Note:** This template provides 1 through 20 separate rows for adding multiple choices.

The Template Sharing Template

The Template Sharing template (`TemplateSharing-template.CSV`) lets you share templates with specific Groups.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Template Name	50	Specify a name for your template to uniquely identify it from other existing templates.
Template Facility	50	Specify the name of the facility in the **Facility 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.
Group Name	50	Specify the name of the Group with which the templates are shared.
Group Facility	50	Specify the name of the Facility associated with the Group with which the templates are shared.

The Template Selected Group Template

The Template Selected Group template (`TemplateSelectedGroup-template.CSV`) lets you add groups to selected groups.

The following table describes the fields names, maximum length for fields names, and a brief description of the fields.

Field	Maximum Length	Description
Template Name	50	Specify a name for your template to uniquely identify it from other existing templates.
Template Facility	50	Specify the name of the facility associated with this template. 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.
Group Name	50	Specify the name of the Group with which the templates are shared.
Group Facility	50	Specify the name of the facility associated with the group with which the templates are shared.

Settings

The **Settings** section of the **navigation bar** in the Vocera Platform Web Console allows you to specify system-wide settings and defaults.

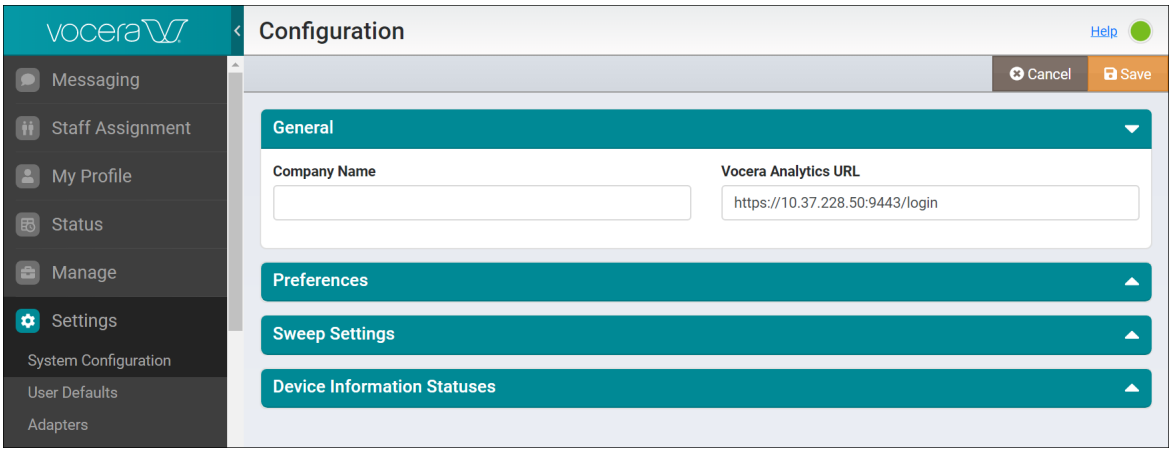
- System Configuration on page 281
- User Defaults on page 291
- Adapters on page 298
- Datasets on page 305
- Workflows on page 309
- Network Settings on page 324
- Voice License on page 329
- Platform License on page 331
- System Backups on page 332
- High Availability on page 351
- Badge Properties Editor on page 367
- Configuration Packages on page 384
- Installed Software on page 388

System Configuration

Specify default settings for the entire Vocera Platform.

These settings are not restricted to a specific facility—they affect the entire Vocera system.

To view the default settings for your system, navigate to the **Settings** section in the Web Console, and select **System Configuration**.



The Configuration page includes the following sections:

- General
- Preferences
- Sweep Settings
- Device Information Statuses

You can click and expand each section to view the system settings and other related details.

General Configuration

Specify your company's name and Vocera Analytics URL.

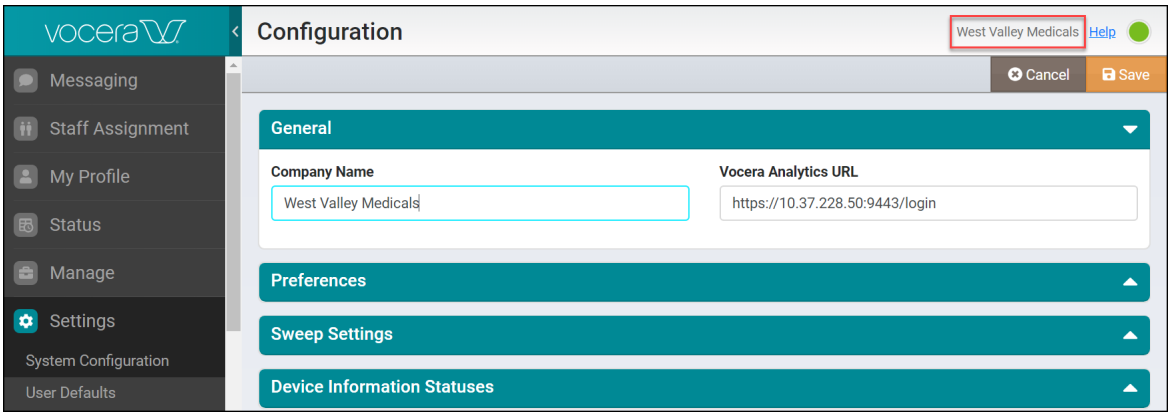
Add general information related to your company name and Vocera Analytics URL (if applicable).

1. Navigate to **System Configuration** in the **Settings** section.
   The Configuration page displays.
2. In the Generation section, complete the fields listed in the following table:

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.

Field	Maximum Length	Description
Vocera Analytics URL	n/a	If you are using Vocera Analytics, specify the IP address. For security reasons, you must register the address of Vocera Analytics with the Vocera Platform in this manner, or the Vocera Platform prevents Vocera Analytics from downloading data. You must also enter the IP address of the Vocera Platform in the Vocera Analytics console. **Note:** The "http://" or "https://" prefix is a required for an IP address.

3. Click **Save** to save your changes and refresh your browser to view your changes.
   You will notice that the name you entered in the **Company Name** field appears near the Help link in the Web Console.
   For example, the following screenshot shows the name "West Valley Medicals" entered in the **Company Name** and the same name appearing on top of the Web Console



   You can also see the **Analytics** section in the Web Console navigation bar. You can click on **Analytics** in the navigation bar to launch the Vocera Analytics login page.

What to do next:

You can enter your credentials to login to the Vocera Analytics visualization server. The visualization server provides real-time data analysis, trends, dashboards, and reports along with the capability to customize reports.

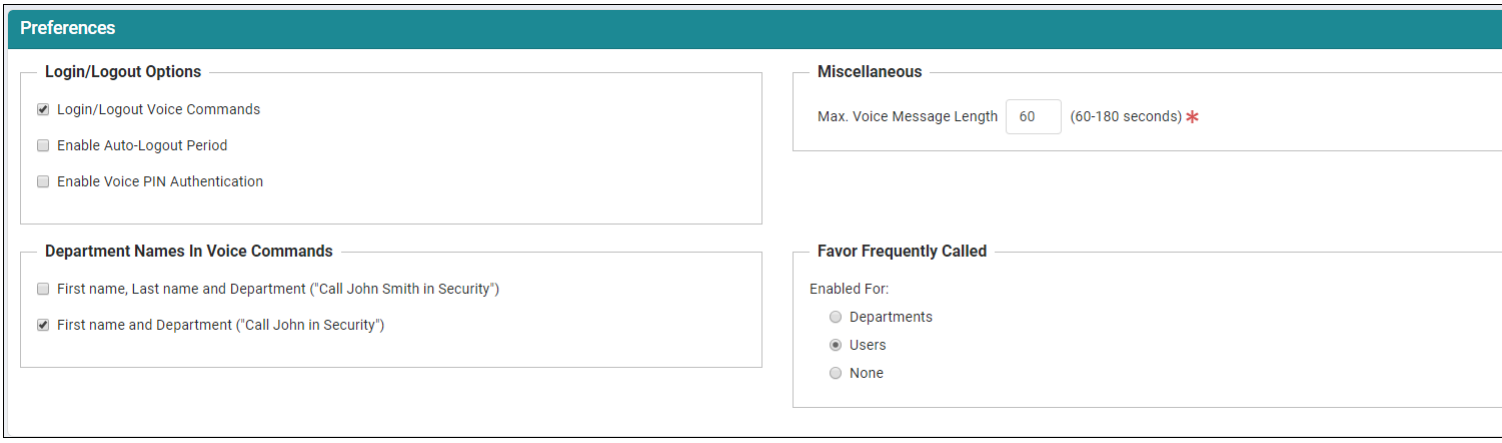
To learn more about Vocera Analytics, refer to the supported Vocera Analytics Administration Guide and other related documents available on the Vocera Documentation Portal.

Setting System Preferences

Set system preferences to establish default settings for the entire Vocera system.

These settings are not limited to a specific facility—they are basic preferences that determine how the entire Vocera system operates.

1. Navigate to **System Configuration** in the **Settings** section of the navigation bar.
2. Scroll down and click on **Preferences** to expand this section.



3. Complete the **Login/Logout Options** configuration fields as described in the following table:

Setting	Description
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 Vocera devices. 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. 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 Vocera devices 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. By default, this setting is not selected.
Enable Voice PIN Authentication	Specifies whether to enable the voice command that allows the users to enter a 5 digit PIN authentication number. This setting is recommended when users want to secure access to voice or text messages using a PIN number. A user can issue a voice command to record or erase a 5 digit PIN number and secure the voice messages. If you disable this command, users cannot enter a PIN number. By default, this setting is not selected.

4. Complete the settings in the **Department Names In Voice Commands** section as described in the following table:

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.

Setting	Description
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 an 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 **Miscellaneous** section as described in the following table:

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.

6. Complete the settings in the **Favor Frequently Called** section as described in the following table:

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 Enabling Favor Frequently Called for Departments or Users on page 285. By default, this setting is not 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 Enabling Favor Frequently Called for Departments or Users on page 285. By default, this setting is selected.
None	Disables the Favor Frequently Called feature for users and departments.

7. Select one of the following:
   - **Save** — to save your changes to the system.
   - **Cancel** — to discard all changes and return to the Configuration page.

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 Voice Service 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 weigh user names and departments in the speech recognition grammars, favoring members of more frequently called users or departments. The call weighing mechanism 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 enabled 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.

Best Practices for Frequently Called Departments

Take full advantage of the Frequently Called Departments feature to improve overall speech recognition using the Vocera recommended 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 in **Preferences** in **System Configuration** in the Web Console. See Setting System Preferences on page 283 for complete information.
3. Define your **Departments** in **Facilities** section of the Web Console.
4. 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.

Enabling Favor Frequently Called for Departments or Users

Learn how to enable favor frequently called feature for departments or users.

The Favor Frequently Called feature for departments works best when all the users, whom 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 facility), can use a special grammar file to aid in successful implementation.

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

The list of users in the Favor Frequently Called feature is used to favor or prefer the frequently called members in the voice recognition result. You can enable or disable the Favor Frequently Called feature for users globally in the Preferences section of the **System Configuration** page. You can enable or disable Favor Frequently Called feature for an individual user also. To learn more about enabling or disabling this feature for an individual user, see the Speech Recognition section Adding a User on page 143.

1. Navigate to **System Configuration** in the **Settings** section of the navigation bar.
2. Scroll down and click on **Preferences** to expand this section.
3. Select one of the following:
   - **Enable for Departments** — to enable Favor Frequently Called feature for departments
   - **Enable for Users** — to enable Favor Frequently Called feature for users in the system
   - **None** — to disable the Favor Frequently Called feature for users and departments
4. Select one of the following:
   - **Save** — to save your changes to the system.
   - **Cancel** — to discard all changes and return to the Configuration page.

Collecting Call Statistics for Frequently Called Departments

For each department group, the Voice Service 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.

Setting Sweep Options

The sweep feature settings allow the Voice Service to clean up voice messages, text messages, and email messages at regular intervals.

You can specify sweep settings so that when a sweep occurs, the Voice Service performs the following tasks:

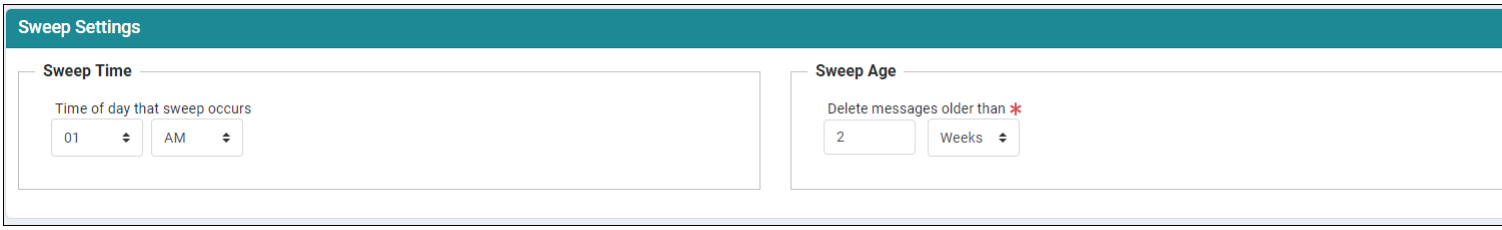
- Delete messages regardless of whether the user has played or read them, unless they have been saved.
- Delete all information about a temporary user from the database.

The sweeps are permanent—users cannot access messages after the Voice Service sweeps them. Similarly, temporary users who have been removed, cannot log in after a sweep occurs.

Independent of the sweep mechanism, the Voice Service 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 Voice Service deletes the oldest unsaved message.
- Each user can **save** up to ten of the 20 stored messages.

1. Navigate to **System Configuration** in the **Settings** section of the navigation bar.
2. Scroll down to the **Sweep** section, and click to expand this section.



3. Enter sweep settings as described in the following table:

Section	Description
Sweep Time	Specify the time of the day when you want the sweep to occur. The default sweep time is 1 a.m.
Sweep Age	Specify the amount of time you want to elapse before the Voice Service 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.

4. Select one of the following:
   - **Save** — to save your changes to the system.
   - **Cancel** — to discard all changes and return to the Configuration page.

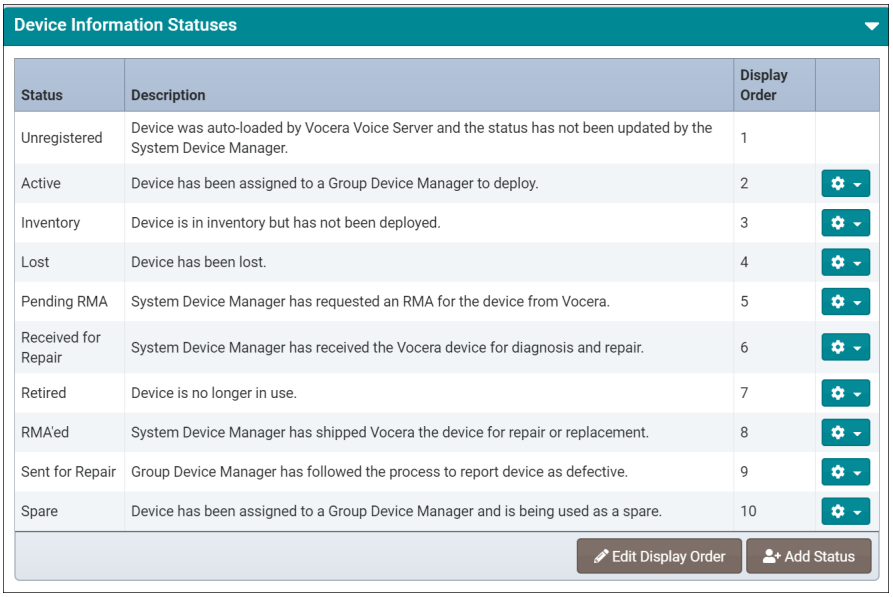
Viewing Device Information Statuses

Learn about the status values for Vocera devices.

Note: Only system administrators and system device managers can add, edit, and delete device status values.

You can define any number of other status values based on the device management processes you have implemented. In the **Device Information Statuses** section, you can add, edit, and delete device status values. You can also change the order of device status values.

Navigate to **System Configuration** in the **Settings** section and scroll down to Device Information Statuses section.



The following table lists the default status values for devices:

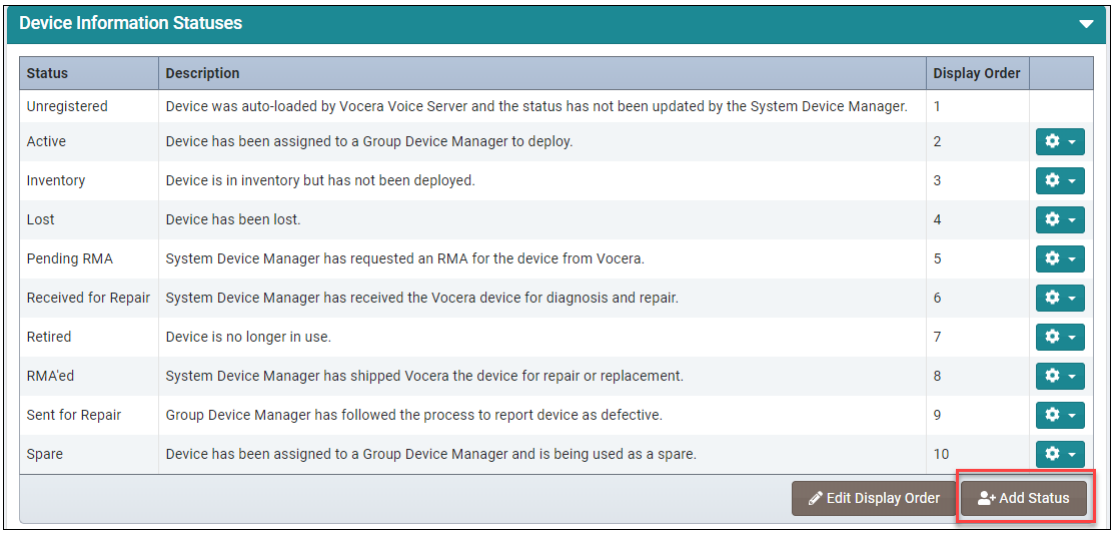
Status	Description
Unregistered	Device was auto-loaded and the status has not been updated by the System Device Manager. **Note:** This status value cannot be deleted or modified.
Active	Device has been assigned to a Group Device Manager to deploy.
Inventory	Device is in inventory but has not been deployed.
Lost	Device is 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 the device to Vocera 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.

Adding a Device Status

Add the device status values based on the device management processes implemented in your organization.

Note: Only system administrators and system device managers can add the device status values.

1. Navigate to **System Configuration** in the **Settings** section of the navigation bar.
2. Scroll down to the **Device Information Statuses** section.
3. Click **Add Status** at the bottom of the **Device Information Statuses** section.



The Add Status dialog box appears.

4. Complete the configuration fields listed in the following table:

Field		Description
Status*	20	Enter a unique name for a new device status.
Description*	100	Enter a brief description of the device status, indicating what the status means and who has this device.

5. Select one of the following to close the dialog:
   - **Done** — to save changes and return to the Configuration page.
   - **Cancel** — to close the Add Status dialog box without saving any changes.

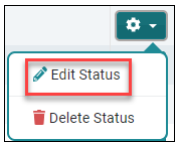
Editing a Device Status

Edit the device status values based on the device management processes implemented in your organization.

Note: Only system administrators and system device managers can edit the device status values.

1. Navigate to **System Configuration** in the **Settings** section of the navigation bar.
2. Scroll down to the **Device Information Statuses** section and click on a device value.
3. Locate the device status value that you want to edit.
4. Choose one of the following:
   - Click on the device status entry that you want to edit to display the Edit Status dialog box.
   - Click the **Options** button on the far right of this entry.

1. Select **Edit Status** from the dropdown menu in the **Options** button.



2. The Edit Status dialog box displays.

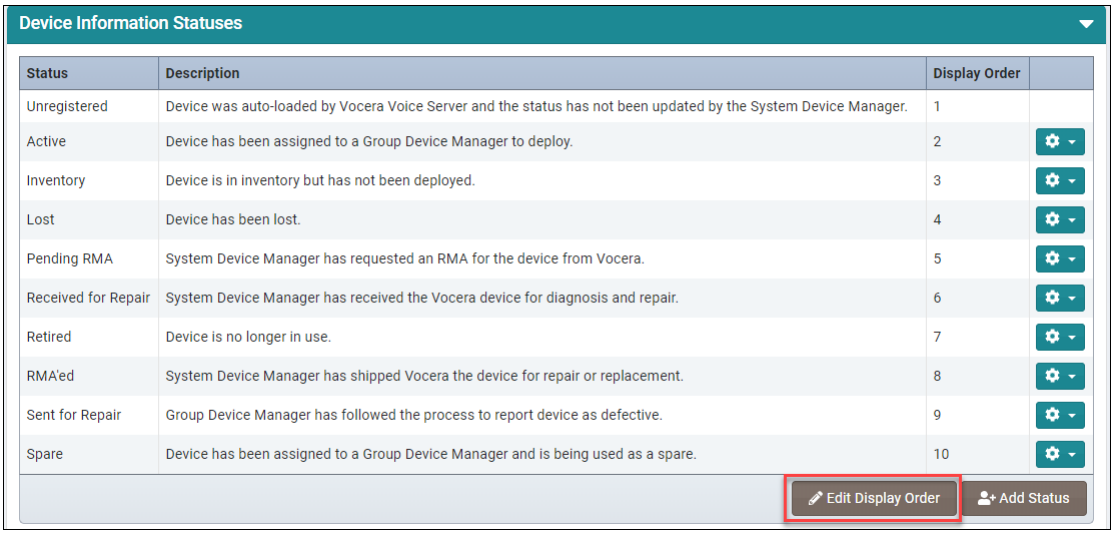
5. Edit the following field information as necessary. See Adding a Device Status on page 288 for a description of the configuration fields.
6. Select one of the following to exit the Edit Status dialog:
   - **Done** — to save changes and return to the Configuration page.
   - **Cancel** — to close the edit dialog box without saving any changes.

Reorder Device Status Values

Reorder the device status values based on the device management processes implemented in your organization.

Note: Only system administrators and system device managers can reorder the device status values.

1. Navigate to **System Configuration** in the **Settings** section of the navigation bar.
2. Scroll down to the **Device Information Statuses** section and click on a device value.
3. Click **Edit Display Order** button at the bottom of this section.



4. Click on the upward and downward arrows in the **Display Order** column to move up or move down the status.

Note: You cannot change the first status value, which is “Unregistered”.

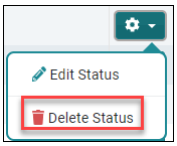
Delete Device Status Values

Delete the device status values based on the device management processes implemented in your organization.

Note: Only system administrators and system device managers can delete the device status values.

1. Navigate to **Settings** in the **System Configuration** section of the navigation bar.
2. Scroll down to the Device Information Statuses section.
3. Select a value in the **Device Information Statuses** list.

   Remember: You cannot delete or modify the "Unregistered" status value
4. Click **Delete Status** from the **Options** button on the far right of the device status that you want to edit.

   The **Delete Status** dialog box appears.
5. Select one of the following to close the dialog:
   - **Yes** — to delete the status and return to Device Information Statuses section.
   - **No** — to close the Delete Status dialog box without deleting the device status.

User Defaults

Defaults are system settings that apply to users at all facilities, 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

Overrides let you establish baseline system settings at any time.

Changes to system defaults update the Vocera Platform Voice Service as soon as you save them, but they do not affect existing users unless you set the **Override User Settings** to **Yes**.

By default, **Override User Settings** is set to **No** for all default settings.

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.

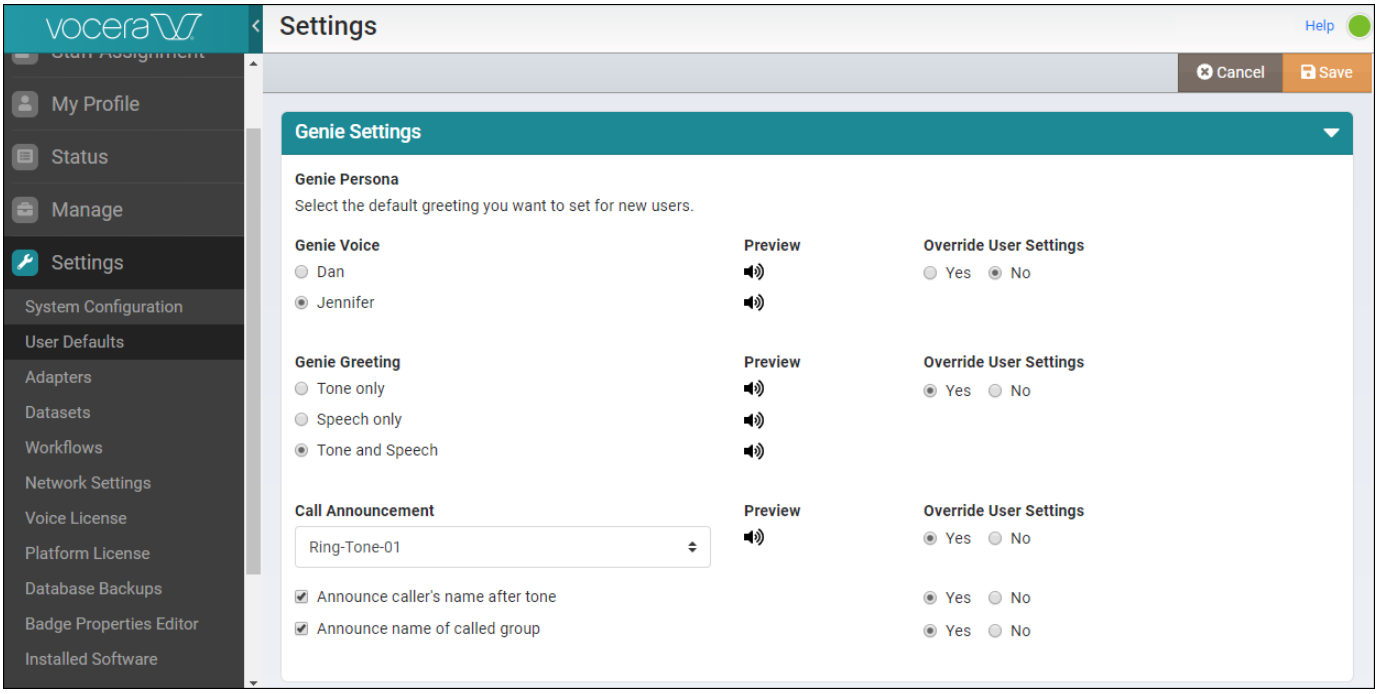
If you later want to allow users to customize this property, set **Override User Settings** for the **Text Message Alert** property to **No**. The alert tones for all users remain turned off until they manually enable them again.

Specifying Genie Settings

The Genie is the voice interface between the user and the Vocera Platform. When a user presses the **Call** button on a Vocera device, the Genie enunciates a greeting, accepts commands, and when necessary, prompts the user. When a call or a voice message is received by a Vocera device, the Genie notifies the recipient.

To specify Genie settings:

1. Click **User Defaults** in the Settings section of the navigation bar. The Genie Settings page displays.



This Settings page includes three sections:

- Genie Settings
- Notification & Miscellaneous Settings
- Initial Passwords

Remember: You can click the drop down arrow at the right hand side of each section to expand or collapse these sections.

2. In the Genie Settings section, set the options listed below. For each option, set **Override User Settings** to **Yes** if the system default for that option takes precedence over a user preference, or to **No** if users can customize the setting you specify.

Field	Description
Genie Voice	Click a radio button to choose a persona for Genie voice. You can click the preview icon by a persona name to play a sample. A Genie voice is a set of voice prompts and tones that give the voice interface a distinctive identity. The default **Genie Persona** varies per locale, and **Override User Settings** is set to **No**
Genie Greeting	A device 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** • **Tone and Speech** Click the icon next to the choice to play a sample greeting. By default the **Speech only** option is selected, and **Override User Settings** is set to **No**
Call Announcement	In the **Call Announcement** section, choose a **Ring Tone** from the list. Click the icon next to the Ring Tone selector 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	Select this checkbox if you want the user to hear who is calling. This announcement adds to the time required to connect each call. By default, the **Announce Name of Called Group** box is selected, and **Override User Settings** is set to **No**.

Field	Description
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 facility to which this group belongs (if it is different from the caller's facility) 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 facilities, the Genie says, "Call to [GroupName] at [FacilityName] from [CallerName]. Accept?" By default, the **Announce Name of Called Group** box is selected, and **Override User Settings** is set to **No**.

3. Specify whether to override any user settings. See Overriding User Settings on page 291.
4. In the Notifications & Miscellaneous Settings section, specify additional notifications and settings. See Specifying Notifications and Miscellaneous Settings for more information.
5. In the Initial Passwords section, specify the initial passwords for user as described in Specifying Initial Passwords.
6. Select one of the following to close the dialog:
   - **Save** — to save your Genie Settings changes to the system.
   - **Cancel** — to discard all changes.

Specifying Notifications and Miscellaneous Settings

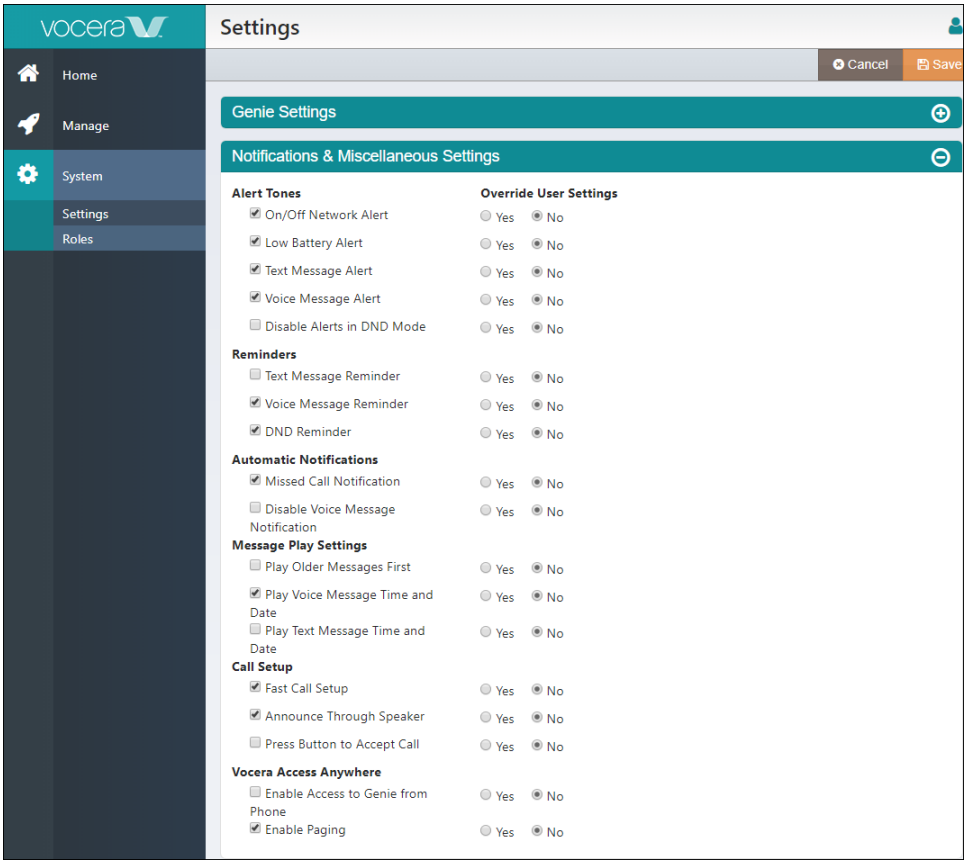
Notifications and Miscellaneous settings control the behavior of the alert tones, reminders that devices play and determine which automatic device features are enabled in user profiles.

Miscellaneous settings control the behavior of the "Play Messages" commands, the behavior of call setup, and the enabling of Vocera Access Anywhere.

To specify notifications and system settings:

1. Navigate to **User Defaults** in the **Settings** section, and click and expand the **Notifications & Miscellaneous Settings**.

   For each checkbox, set **Override User Settings** to **Yes** if the system default for that checkbox takes precedence over a user preference, or to **No** if users can customize the setting you specify. See Overriding User Settings on page 291 for more information.



a. Specify alert tone settings in the **Alert Tones** section:

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 Alerts in DND Mode	**Disable Alerts 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 not selected, and **Override User Settings** is set to **No**.

b. Choose any reminders you want to enable in the **Reminders** section:

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 not selected, 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**.

c. Choose any notifications you want to enable in the **Automatic Notifications** section. Automatic notifications allow users to bypass certain operations without confirming them.

Setting	Description
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. Users may prefer to use the "Who called?" command when they are in a quiet area to learn who called. If users are trained to do that, you can clear the **Missed Call Notification** setting. 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 not selected, and **Override User Settings** is set to **No**.

d. In the **Message Play Settings** section, specify the behavior of the "Play Messages" commands.

Setting	Description
Play Older Messages First	**Play Older Messages 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 not selected, 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 not selected, and **Override User Settings** is set to **No**.

e. In the **Call Setup** section, specify the behavior of the call setup.

Setting	Description
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, "Can you talk to [*CallerName*]?" 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**.
Press Button to Accept Call	Use the **Press Button to Accept Call** setting to require 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 accept or reject calls without user input prematurely. To avoid these problems, select this box to require users to answer calls using buttons only. By default, the **Press Button to Accept Only** box is not selected, and **Override User Settings** is set to **No**. Enabling this feature establishes a new system-wide default and may require re-training.
Enable Paging	Enable the Vocera Access Anywhere paging capability. By default, the Enable Paging box is selected, and Override User Settings is set to **No**.

2. In the **Frequently Called User Settings**, select the **Enable Frequently Called User** checkbox Selecting the **Enable Frequently Called User** checkbox allows the use of call history data for calls made to a circle of frequently called users to enhance speech recognition for the Vocera system
3. In the Vocera Access Anywhere section, select the **Enable Vocera Access Anywhere** checkbox 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.
4. Specify whether to override any user settings. See Overriding User Settings for more information.
5. Select one of the following to close the dialog:
   - **Save** — to save your Notifications & Miscellaneous Settings Settings changes to the system.
   - **Cancel** — to discard all changes.

Specifying Initial Passwords

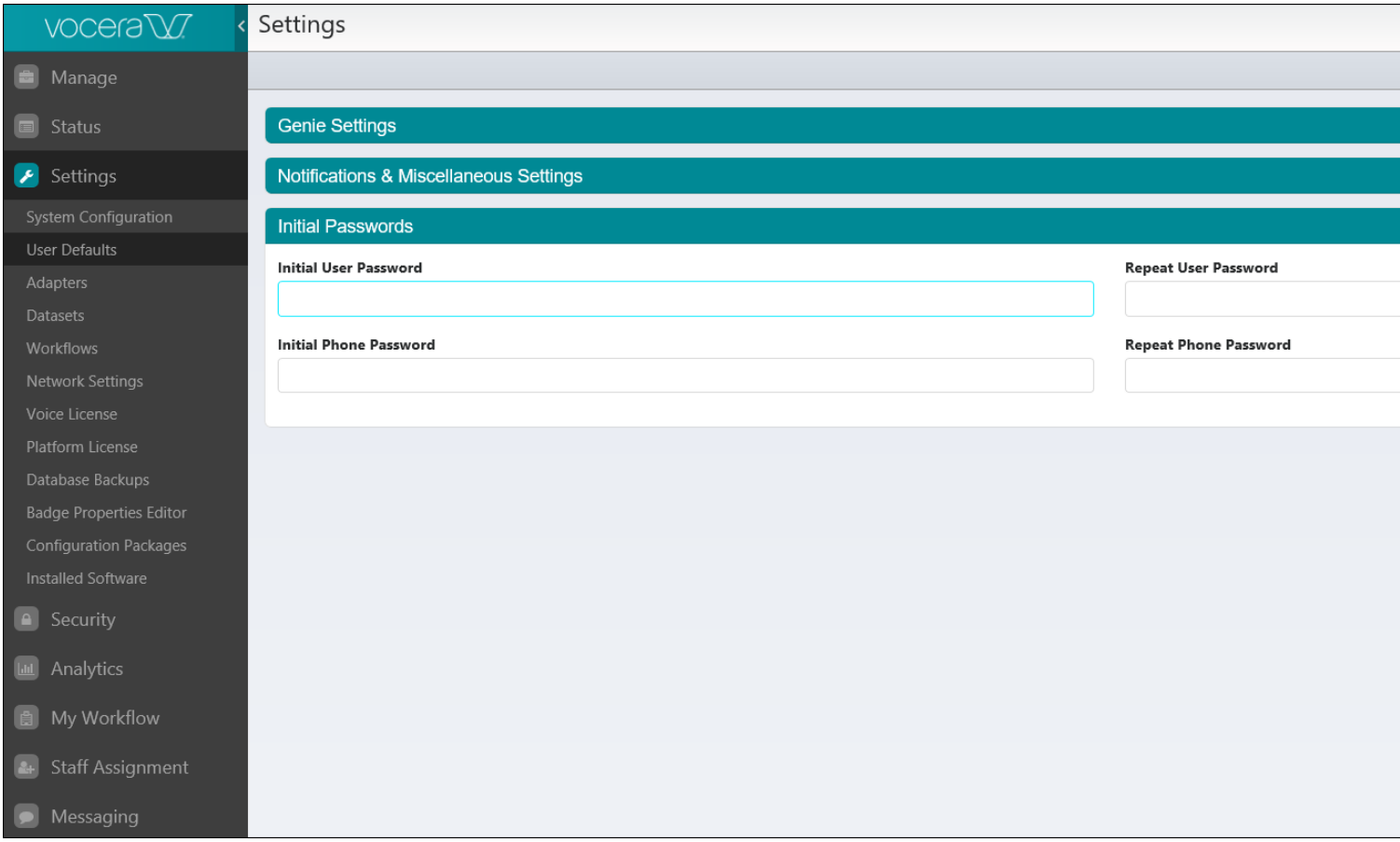
Initial user password provides a default password for each new user account.

Users can specify this password to gain access to the Vocera Platform Web Console the first time they log in. Users can then change this initial password.

By default, the **Initial User Password** field is blank. That is, users do not have to provide a password the first time they log in to the Vocera Platform Web Console.Users who are enabled to access the Genie from a phone must specify a phone password if Caller ID is not supported.

To add an initial password:

1. Click **Initial Passwords** in the **User Defaults** section.



2. Enter a value for the **Initial User Password** and **Initial Phone Password** fields.
   You must also enter the same value in the **Repeat User Password** and **Repeat Phone Password** fields.
3. Select one of the following to close the dialog:
   - **Save** — to save the initial passwords in the system.
   - **Cancel** — to return to the Settings page.

Adapters

The Vocera Platform uses adapters to integrate with external systems and devices.

You can configure each adapter to include information that allows Vocera Platform to communicate and interact with a specific type of resource, and the devices that resource may control. Adapters can allow the Vocera Platform to monitor and collect data as well as send data out when triggered manually or automatically.

If not provided by default in a Vocera Platform EMDAN solution, an adapter package can be manually implemented. The adapter package has to be uploaded to Vocera Platform, and then installed and configured. Once the adapter configuration is enabled, Vocera Platform can utilize the adapter's functionality. Multiple instances of an adapter can be created in Vocera Platform.

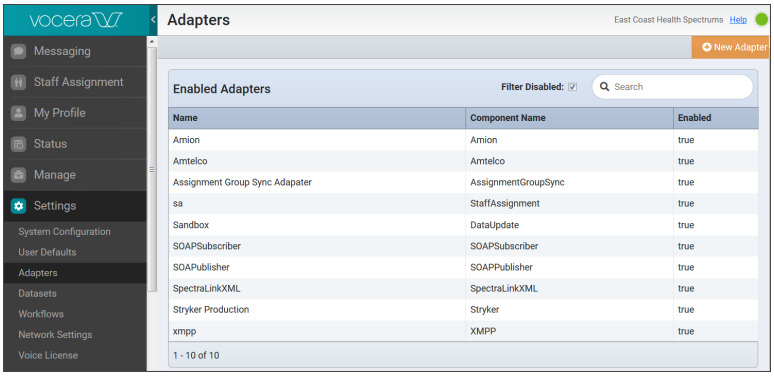
Note: For details about adapters, navigate to the indvidual adapter guides listed under Vocera Adapters in the Vocera Documentation Portal. Each guide contains installation and configuration details, as well as instructions for creating, enabling, deleting, and editing adapters.

An adapter's service status can be verified or enabled in **Status > Adapter Services**.

Note: For information about **Adapter Services**, see the Status on page 96 section of this Vocera Platform Administration Guide.

In the Vocera Platform Web Console navigation menu, select **Settings**, then **Adapters**.

The **Adapters** page displays a list of adapters installed on the Vocera Platform. On this page you can identify installed adapters by component or reference name. The adapter list can be filtered by a search term, or by enabled status. In addition, from this page you can choose to create a new adapter instance.

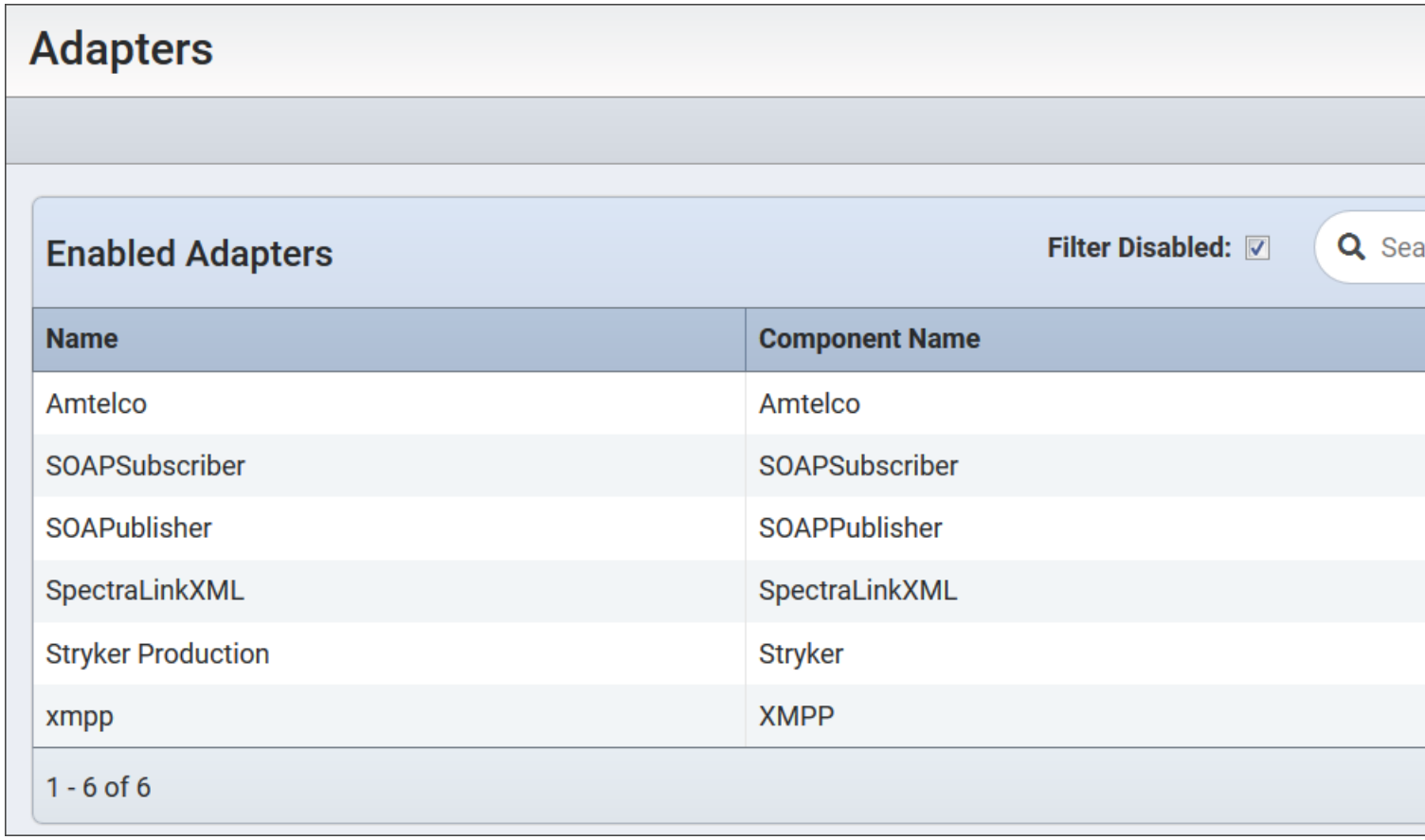


Accessing the Adapters List

View the list of adapters installed on the Vocera Platform and their current enabled status.

The Adapters page provides a list of installed adapters, and their enabled status in a table. The number of displayed adapters is shown in the table's footer. Click a name in the Adapters list to enable that adapter, or to edit other configuration fields as needed. From this page you can also create a new adapter.

1. Navigate to **Adapters** in the **Settings** section of the Vocera Platform Web Console.
   The Adapters page displays.
2. View the list of adapters in the **Adapters** table.



3. The **Adapters** table provides the following information:

Feature	Description
Name	This is the name of the adapter instance created on the Vocera Platform. Unique and descriptive names should be created when multiple adapter instances are needed. See the Reference Name description for the adapter to install.
Component Name	This is the name of the installed Vocera component.
Enabled	This indicates whether the adapter instance is enabled and available on the Vocera Platform. An adapter instance can be created, but it will not be available to Vocera Platform until Enabled is checked in the adapter's configuration settings.

Feature	Description
Filter Disabled	Select the **Filter Disabled** checkbox in the table's header to toggle between views which display **All Adapters** and **Enabled Adapters**. This box is checked by default, filtering the list to display only enabled adapters. When the **Filter Disabled** box is checked, the list of adapters in this page is restricted to adapters enabled for processing on Vocera Platform. When the box is unchecked, all installed adapters are displayed in the list.
Search	Enter an adapter search term in the **Search** field in the table's header to filter the adapter list. Search terms will be applied to the Name and Component Name fields. When all adapters configured on Vocera Platform are shown, the header displays **All Adapters**. When a search has limited the number of adapters shown, the header displays **Adapters Search Results**. Search controls include a magnifying glass icon to initiate the search, and an "x" icon to clear the search field. The search term is autosubmitted after the user pauses in typing.

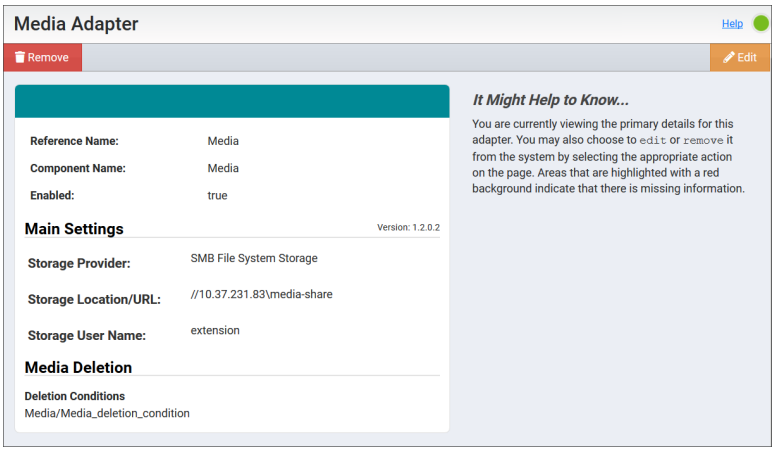
4. Click a name in the Adapters list to view its details. See Viewing Adapter Configuration Details on page 300 for more information.
5. Click **New Adapter** to create a new adapter on Vocera Platform. See Creating a New Adapter on page 301 for details.

Viewing Adapter Configuration Details

Select a name in Adapters to display the adapter's configuration details.

Note: For configuration details, navigate to the indvidual adapter guides listed under Vocera Adapters in the Vocera Documentation Portal.

1. Navigate to **Adapters** in the **Settings** section of the Vocera Platform Web Console.
   The Adapters page displays.
2. Select an adapter name in Adapters.
   The adapter's configuration settings display.
3. View the configuration details for the selected adapter.



4. Use the information in the following table to understand the adapter details provided.

Note: This section describes the configuration elements that are required for all adapters. See an adapter guide to view the configuration specific to that adapter.

Field	Description
Name	This is the name of the adapter instance created on the Vocera Platform. Unique and descriptive names should be created when multiple adapter instances are needed. See the Reference Name description for the adapter to install.
Component Name	This is the name of the installed Vocera component.
Enabled	This indicates whether the adapter instance is enabled and available on the Vocera Platform. An adapter instance can be created, but it will not be available to Vocera Platform until Enabled is checked in the adapter's configuration settings.

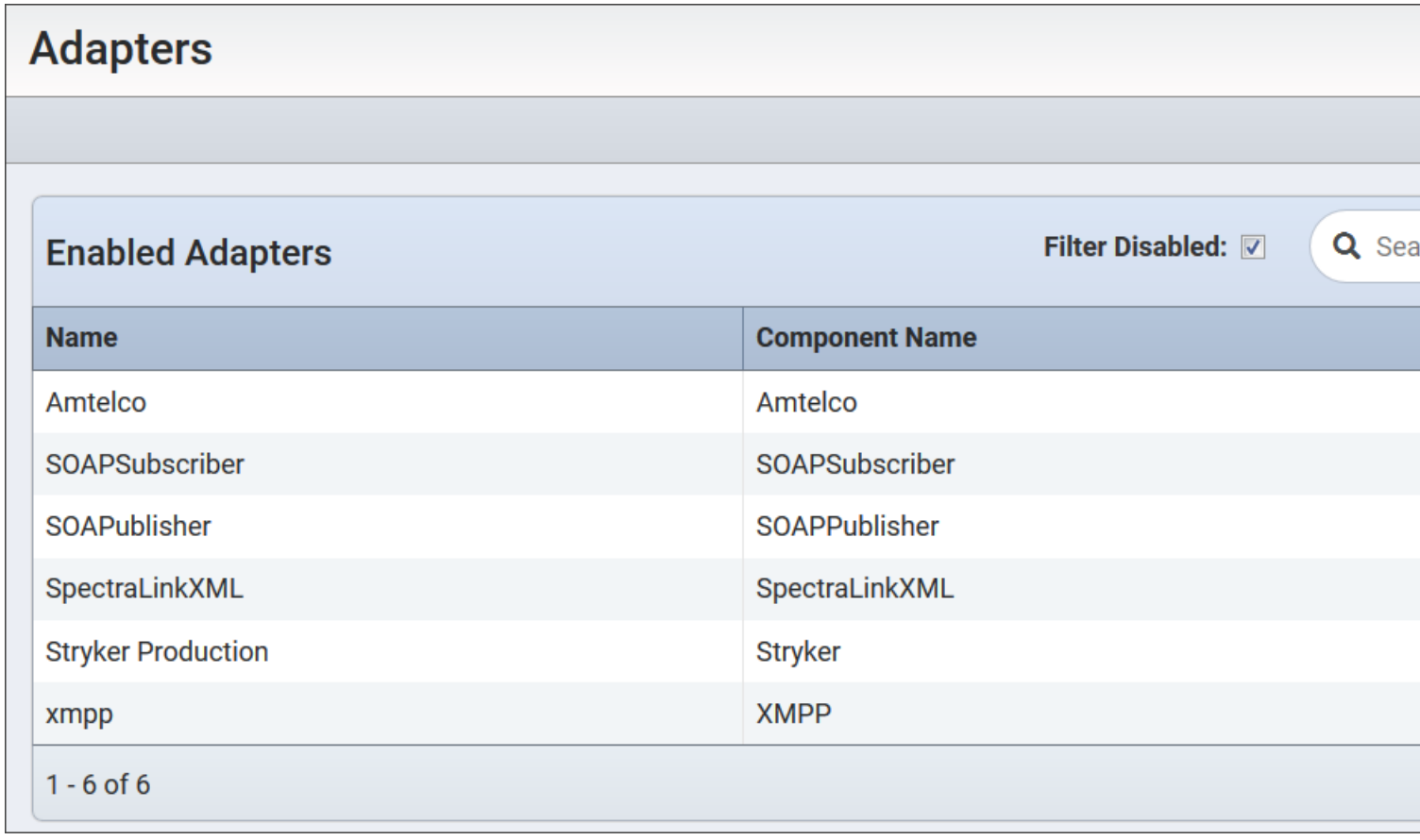
5. Choose one of the following menu options as needed.
   - Select **Edit** to revise the configuration of the selected adapter.
   - Select **Remove** to delete the selected adapter from the Vocera Platform.

Creating a New Adapter

Once an adapter component is installed, create an instance of that adapter in Vocera Platform.

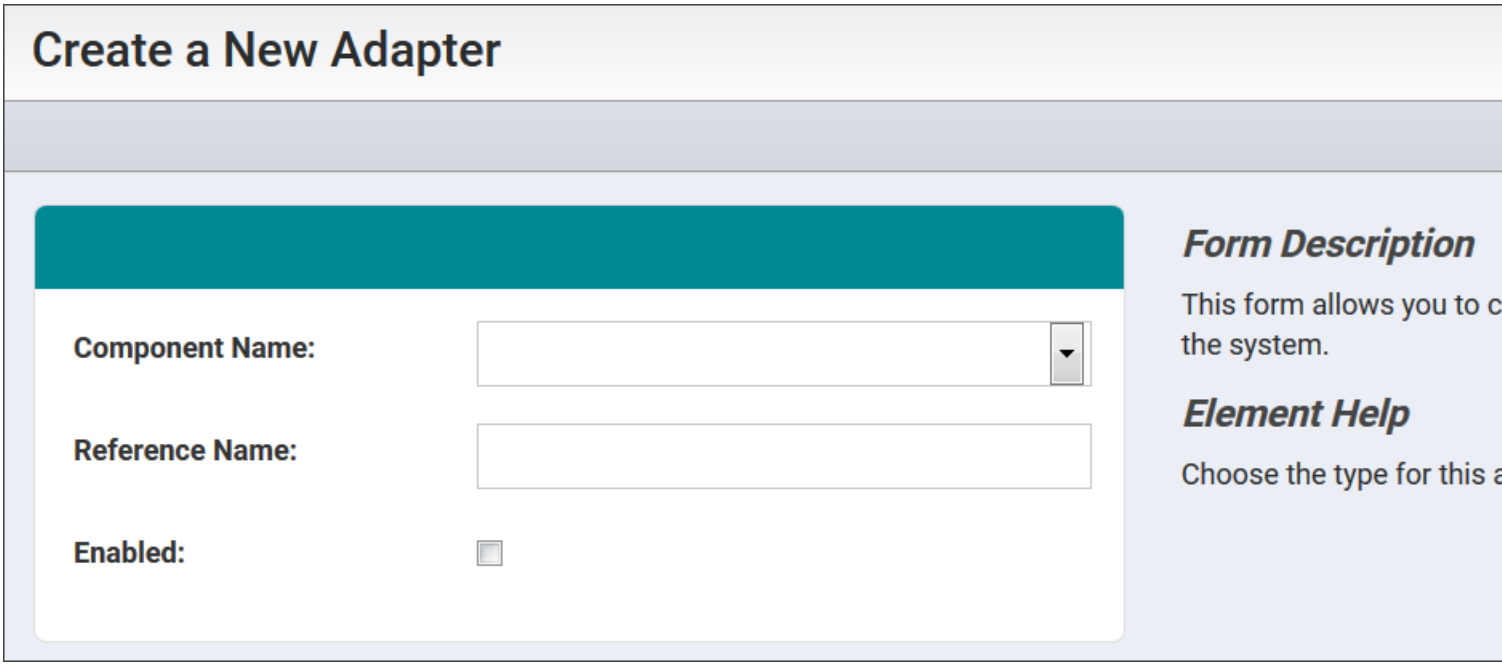
For configuration documentation, see the indvidual adapter guides listed in Vocera Adapters in the Vocera Documentation Portal. Each adapter's configuration guide describes the information that must be provided in the configuration fields for that adapter. In addition, the recommended best practice installation steps are provided in each adapter guide.

1. Select **New Adapter** in the Adapters page.



The Create a New Adapter page displays.

2. In the **Create a New Adapter** page, you can select an installed adapter component to implement. An option is also provided to upload an adapter bundle to Vocera Platform; see Uploading a Bundle on page 302 for an explanation of this functionality.



3. Select an adapter in the Component Name dropdown list to display the configuration fields for that component. The Reference Name field and the Enabled checkbox are common to every adapter, and are described in this table.

   When the component name is selected, additional fields display which are unique to the selected adapter; these configuration options are described in the adapter's configuration guide.

Feature	Description
Component Name	Click the Component Name field to display a list of installed adapters. Select the name of the adapter to create on the Vocera Platform. The configuration fields specific to the adapter will display below the Enabled checkbox. See the Vocera Adapters documentation for adapter-specific configuration details.
Reference Name	Enter a short descriptive name in the Reference Name field to uniquely identify an adapter instance. See the Vocera Adapters documentation for adapter-specific configuration details.
Enabled	Select the Enabled checkbox to allow the Vocera Platform to use the new adapter. An adapter instance can be created, but it will not be available to Vocera Platform until Enabled is checked in the adapter's configuration settings. See the Vocera Adapters documentation for adapter-specific configuration details.

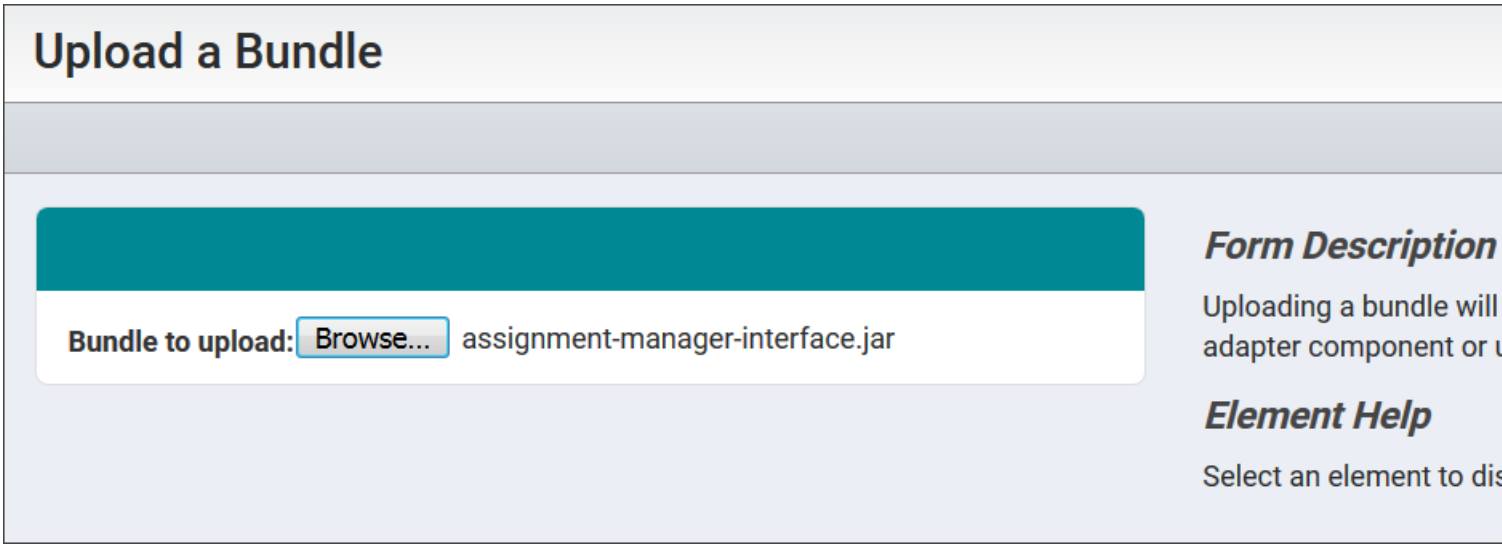
Uploading a Bundle

Uploading an adapter bundle through the Vocera Platform Web Console is required only in specific circumstances. Vocera recommends calling **Customer Support** if you need to upload a bundle.

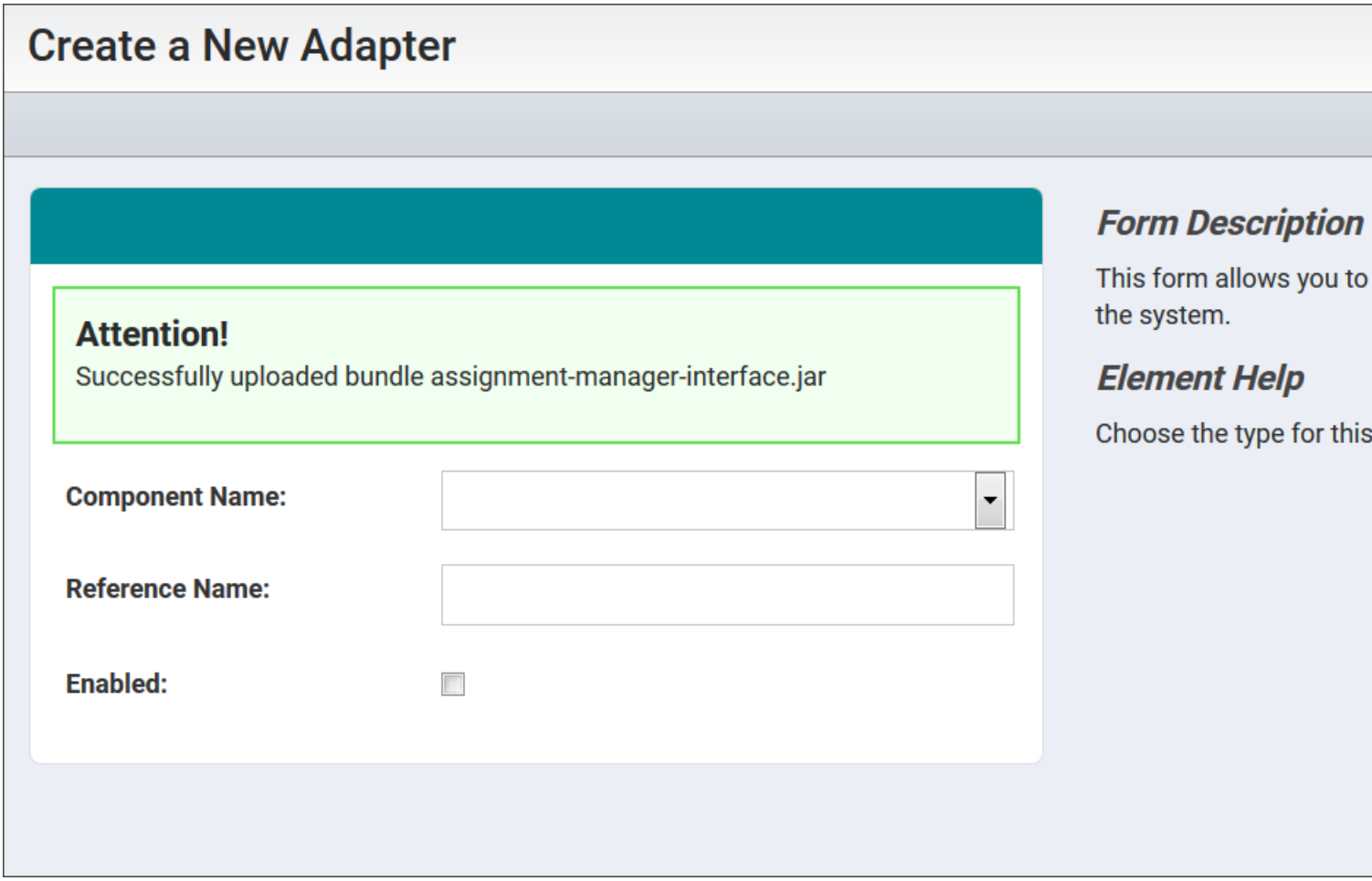
Use the Upload Bundle feature to install an adapter when it is not available in the Component Name dropdown list, and you have downloaded the needed adapter bundle to a storage location.

See the recommended best practice for uploading an adapter component in the **Installation** content found in each adapter guide in Vocera Adapters.

1. Click **Upload Bundle** in the Create a New Adapter page to add an adapter component to Vocera Platform. See Creating a New Adapter on page 301 for access to the upload option.
   The Upload a Bundle page displays.
2. Browse to the location where the adapter component bundle is stored.



   Choose one of the following:
   - Cancel—Return to the Create an Adapter page without uploading an adapter bundle.
   - Upload—Upload the selected bundle to Vocera Platform.
3. Click **Upload** in the Upload a Bundle page to add the adapter component to the Vocera Platform.



The Create a New Adapter page displays with a success message; on this page you can complete the configuration for the uploaded adapter component. An error message displays if the upload is unsuccessful.

4. Configure the newly installed adapter component. See Vocera Adapters for the specific adapter guides. When complete, select one of the following options to exit.
   - Select Upload Bundle to implement another adapter component.
   - Use the Vocera menu to navigate away from the Create a New Adapter page.

Datasets

Datasets allow Vocera to store and refer to a large amount of contextual data, such as data about users, groups, devices, templates, and more to generate alerts and notifications.

The Vocera datasets are defined by their purpose (such as NurseCalls, Deliveries, or Conversations), and are built to house specific pieces of data in their attributes while also using links to connect to other datasets. For example, when an alert is triggered and processed, data is added to many attributes on a number of different datasets in order to provide the proper processing and context for the alert.

Datasets may link to other datasets and allow linked attribute access across two or more datasets. For example, an alert is linked to a patient, room, and bed in order to display this information on the user's device when the alert is triggered. Each of these respective attributes are housed in separate datasets. Attributes, Conditions, and Rules configured on a dataset are used to manage this information. You can create attributes to display within messages if the correct conditions are met and a rule empowering the action is triggered.

The **Datasets** section in the Vocera Platform Web Console provides access to the datasets configured on the Vocera Platform. The default view displays a list of datasets, alphabetically ordered by name, accompanied by a brief description. You can enter a dataset name or description in the search field to find a specific dataset or narrow the search results. Using the functionality in Datasets, you can create a new dataset or work with the configurable elements (such as conditions, filters, and attributes) of an existing dataset in the Vocera Platform.

A System Administrator may be authorized to work with Vocera's dataset functionality. In the Vocera Platform Web Console users may be authorized to create, delete, modify, and publish datasets.

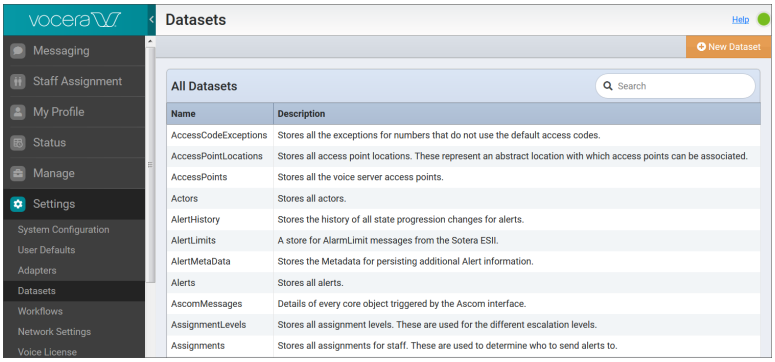
Accessing the Datasets List

View a list of datasets configured on the Vocera Platform, or use the search bar to display a specific dataset.

Datasets are organized alphabetically by name in a table. The number of implemented datasets is shown in the table's footer.

To access the Datasets lists, follow these steps:

1. Navigate to **Datasets** in the **Settings** section of the Web Console.
   The Datasets page displays.



2. Use the following table to understand the details provided in Datasets.

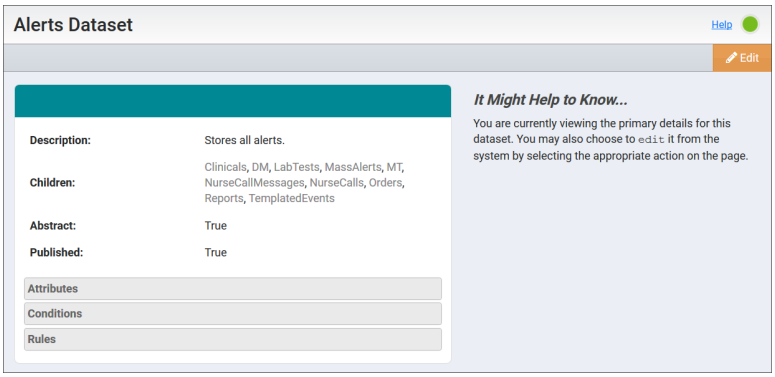
Feature	Description
Name	Specifies the name of the dataset created on the Vocera Platform.
Description	Describes the purpose or other unique details relevant to the dataset.
Search	Enter a term in the **Search** field to filter the dataset list. Search terms are applied to the Name and Description fields. The web console search immediately pulls any records matching the dataset name or description that you entered and displays this information. When all datasets configured on Vocera Platform are shown, the header displays **All Datasets**. When a search has limited the number of adapters shown, the header displays **Datasets Search Results**.

Viewing Dataset Configuration Details

View the configuration details for a dataset implemented on the Vocera Platform.

To view the configuration details for a dataset, follow these steps:

1. Navigate to **Datasets** in the **Settings** section of the Vocera Platform Web Console.
   The Datasets section displays.
2. Select a dataset in the list.
   The dataset's configuration page displays.
3. Use the information in the following table to understand the dataset details provided.



Field	Description
Description	Describes the selected dataset's functionality.
Children	Displays the names of all the dependent/children datasets to this parent (Top Level) dataset in the database hierarchy.

Field	Description
Abstract	Indicates whether the dataset is considered abstract. The **Abstract** field can have True or False values. A True value indicates that you cannot store information directly in the dataset. A False value indicates that you can store information directly in this dataset. An abstract dataset is a view of data; it can aggregate data but cannot contain data, and can be specified only when creating a new dataset.
Published	Displays a value of True or False. A True value indicates that the dataset is published and available for use on the system. Do not revise or remove a dataset after it is published. A False value indicates the dataset is not published to the system. This datset may be edited.
Attributes	Regular attributes and link attributes represent data stored on a Vocera dataset. You can expand this option to view the attributes defined on the selected dataset.
Conditions	Conditions provide access to a subset of a dataset when only particular events or records within a dataset are needed. You can e\xpand this option to view the conditions defined on the selected dataset.
Rules	Rules are used to send messages when events occur within the system. You can expand this option to view the rules defined on the selected dataset.

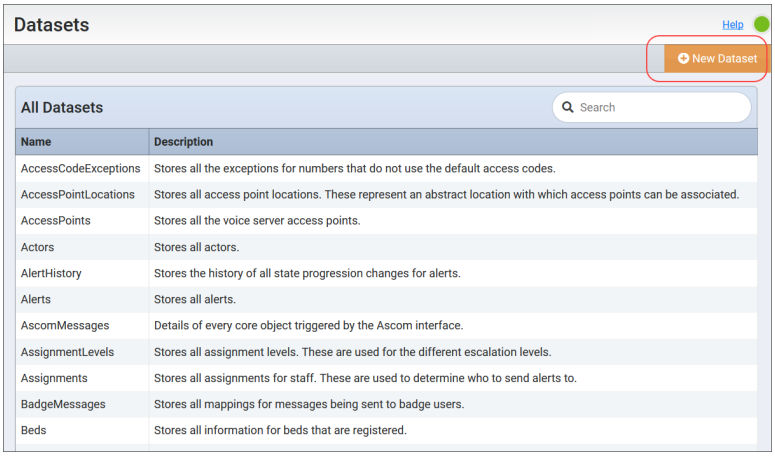
Creating a New Dataset

Complete these configuration fields to create a new dataset on Vocera Platform.

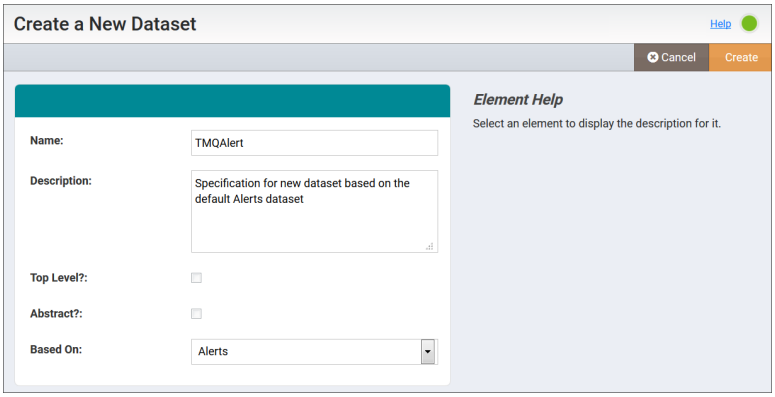
Once you have defined a new dataset as described here, publish the dataset to the Vocera system.

To create a new dataset, follow these steps:

1. Navigate to **Datasets** in the **Settings** section of the Vocera Platform Web Console.
   The Datasets section displays.
2. Select **New Dataset** in Datasets.



The Create a New Dataset page displays.



3. Use the information in the following table to complete the **Create a New Dataset** configuration fields.

Field	Description
Name	Enter a name that identifies the new dataset. The name must begin with a capital letter, and contain no spaces. The new dataset cannot use an existing, published dataset name.
Description	Enter a clear description defining the dataset's purpose.
Top Level?	Select the **Top Level** checkbox if the dataset being created has no parent dataset. Selecting the Top Level checkbox specifies that this dataset will not inherit any data from a parent dataset. Selecting the **Top Level** checkbox enables the **Abstract** checkbox, but disables the **Based On** drop-down menu.
Abstract?	Select the **Abstract** checkbox if you want to use this dataset to define common attributes shared between similar datasets. The **Abstract** checkbox is enabled only when the **Top Level** checkbox is selected.
Based On	Select a previously defined dataset from the **Based On** drop-down menu. Only abstract datasets may be used as the basis for a new dataset. The new dataset will be based on the existing abstract dataset. Using an existing abstract dataset makes the new dataset creation process more efficient if the datasets share many common elements. The **Based On** dropdown list is disabled when the **Top Level** checkbox is selected.

4. • **Save** — to save your Genie Settings changes to the system.
   • **Cancel** — to discard all changes.
5. Select one of the following to exit the Create a New Dataset configuration dialog:
   • **Create** — to add the new dataset to the Vocera Platform.
   • **Cancel** — to return to Datasets without adding a new dataset to the system.

Workflows

Workflows allow users to interact with information stored in the Vocera Platform.

A workflow can contain one or more pages. You can configure a workflow page to display useful information and permit the user to access additional workflows or pages.

You can also configure workflow pages in such a way that users can enter information which can be stored in the Vocera Platform. In other words, workflows allow the system to read and update data from the users. For example, you can utilize workflow pages to store information on staff assignments or phone-to-user assignment details, and manage this functionality through the workflow pages. After configuring a workflow, you can access it from a web browser or third party phones.

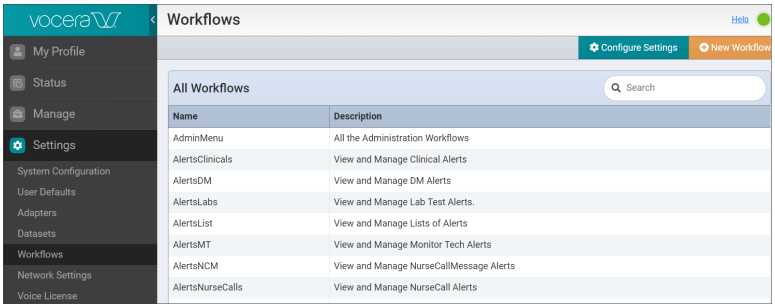
Accessing the Workflows List

View a list of workflows implemented on the Vocera Platform or use the search bar to display a specific workflow.

Workflows are organized alphabetically by name in a table. The number of implemented workflows is shown in the table's footer.

To access the workflows list, follow these steps:

1. Navigate to **Workflows** in the **Settings** section of the Web Console.
   The Workflows section displays.



2. Use the information in the following table to understand the details provided in the Workflows section.

Field	Description
Name	This is the name of the implemented Vocera workflow. The name should be unique and identify the selected workflow's functionality.
Description	This is the description of the selected workflow's purpose. The description of the workflow should be explicit as possible, so users will understand the purpose of the workflow.

Field	Description
Search	Enter a search term in the **Search** field in the table's header to filter the workflow list. Search terms will be applied to the Name and Description fields. When all workflows configured on Vocera Platform are shown, the header displays **All Workflows**. When a search has limited the number of workflows shown, the header displays **Workflows Search Results**. Search controls include a magnifying glass icon to initiate the search, and an "x" icon to clear the search field. The search term is autosubmitted after the user pauses in typing.

Click a name in the Workflows list to view its details. See Managing Workflows on page 311 for more information.

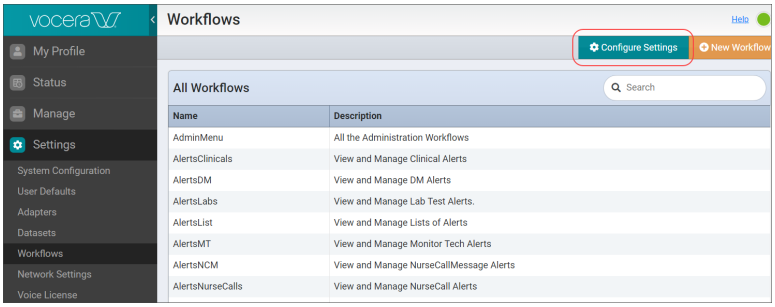
Configuring the Workflows Settings

Define the default stylesheet and browser page display for all workflows.

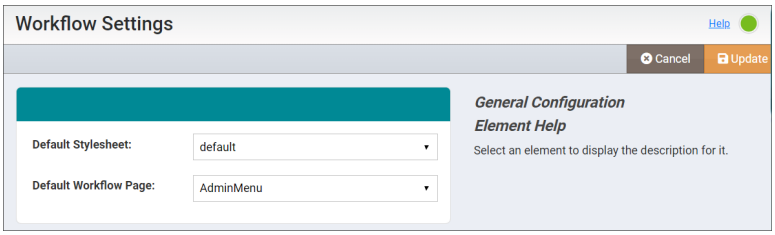
Users with roles that have Advanced Support policies applied can set the default workflow configuration described here.

To configure workflow settings, follow these steps:

1. Select **Configure Settings** in the Workflows menu.



The Workflow Settings page displays.



2. Use the following information to define default settings to apply to all workflows.

Field	Description
Default Stylesheet	Select the stylesheet to display in the web browser of the user's device when a workflow is utilized. The options are: • blank; this option will present the default stylesheet unless a specific stylesheet is configured for an individual workflow. • blue • slate • default; this option presents the configured default stylesheet.

Field	Description
Default Workflow Page	Select the workflow page to display when a workflow is utilized. This option provides a dropdown list of workflows configured on the system. Select one workflow from this list.

3. Select one of the following to exit the Workflow Settings configuration dialog:
   - **Cancel** — to return to the Workflows page without making a change.
   - **Update** — to save the configuration settings to the system.

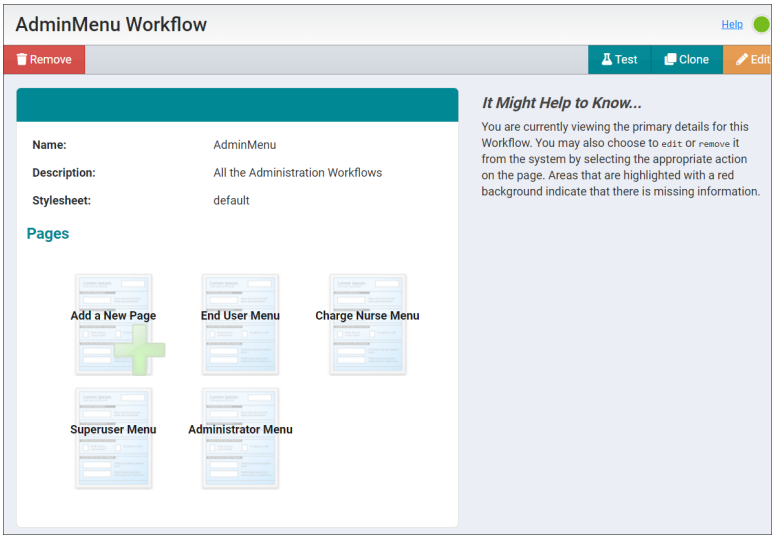
Managing Workflows

View the primary details of a selected workflow, and the options provided to manage a workflow on the Vocera Platform.

Use the options in the menu to revise a selected workflow's pages, test its functionality, remove it from the system, or clone the workflow.

To manage your workflows, follow these steps:

1. Select a workflow from the Workflows list.
   The workflow's details display.
2. Use the information in the following table to understand the workflow details provided.



Field	Description
Name	This is the name of the implemented Vocera workflow. The name should be unique and identify the selected workflow's functionality.
Description	This is the description of the selected workflow's purpose. The description of the workflow should be explicit as possible, so users will understand the purpose of the workflow.

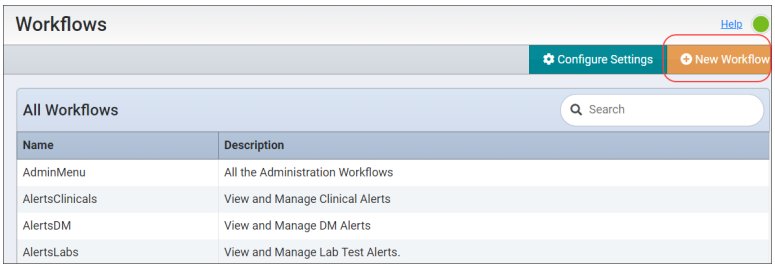
Field	Description
Stylesheet	Select the stylesheet to display in the web browser of the user's device when this workflow is utilized. The options are as follows: • blank; this option will present the default stylesheet unless a specific stylesheet is configured for an individual workflow. • blue • slate • default; this option presents the configured default stylesheet.
Pages	This section contains the configured pages that provide the workflow's functionality, and an **Add a New Page** option. The first page is what is displayed if a user simply accesses the workflow by name, without specifying an individual page. When a workflow is tested, the first page is also what is initially presented to the user. See Working With Workflow Pages on page 317 for additional information.

Creating a New Workflow

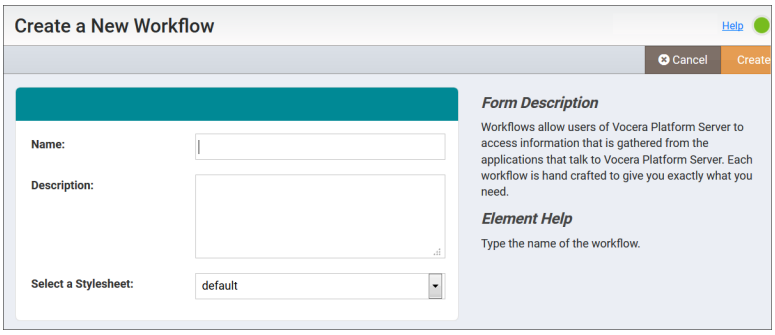
Complete these configuration fields to create a new workflow on Vocera Platform.

To create a new workflow, follow these steps:

1. Select **New Workflow** in the Workflows menu.



The Create a New Workflow page displays.



2. Use the information in the following table to complete the configuration fields when creating a new workflow.

Field	Description
Name	Enter a name that is unique and identifies the selected workflow's functionality.
Description	Enter a description of the workflow's purpose. This should be explicit as possible, so users will understand the purpose of the workflow.

Field	Description
Select a Stylesheet	Select the stylesheet to display in the web browser of the user's device when this workflow is utilized. The options are as follows: • blank; this option will present the default stylesheet unless a specific stylesheet is configured for an individual workflow. • blue • slate • default; this option presents the configured default stylesheet.

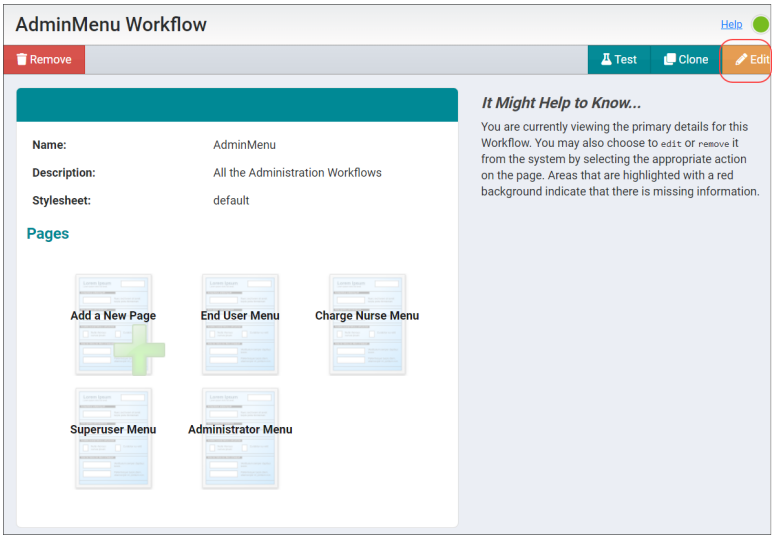
3. Select one of the following to exit the Create a New Workflow configuration dialog:
   - **Create** — to add the new workflow to the Vocera Platform.
   - **Cancel** — to return to Workflows without adding a new workflow to the system.

Editing a Workflow

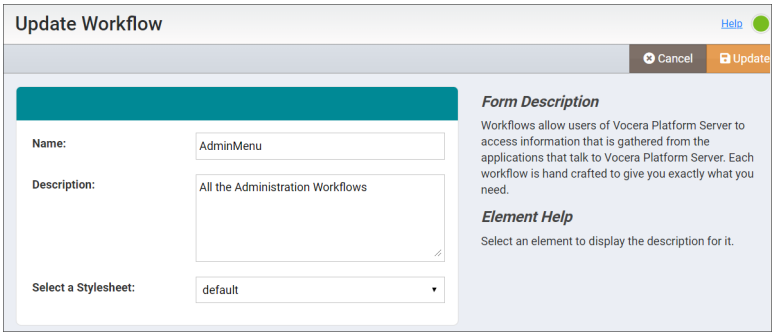
Modify an existing workflow and update it with your changes on Vocera Platform.

To modify an existing workflow, follow these steps:

1. Select a workflow from the Workflows list.
   The workflow's details display.
2. Select **Edit** in the workflow menu.



The Update Workflow dialog displays.



3. Use the information in the following table to complete the configuration fields in the **Update Workflow** dialog.

Field	Description
Name	Enter a name that is unique and identifies the selected workflow's functionality.
Description	Enter a description of the workflow's purpose. This should be explicit as possible, so users will understand the purpose of the workflow.
Select a Stylesheet	Select the stylesheet to display in the web browser of the user's device when this workflow is utilized. The options are as follows: • blank; this option will present the default stylesheet unless a specific stylesheet is configured for an individual workflow. • blue • slate • default; this option presents the configured default stylesheet.

4. Select one of the following to exit the Update Workflow configuration dialog:
   - **Update** — to modify the workflow on the Vocera Platform.
   - **Cancel** — to return to Workflows without adding a new workflow to the system.

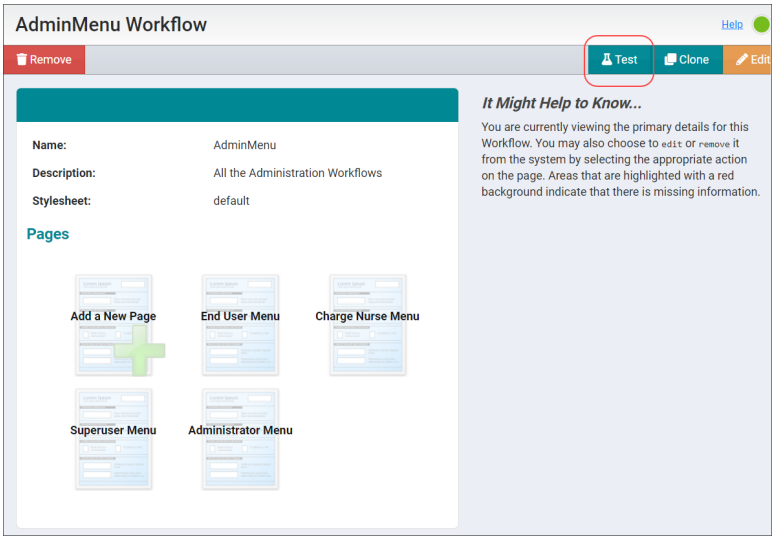
Testing a Workflow

Test the workflow that you created or selected, and verify the results on Vocera Platform.

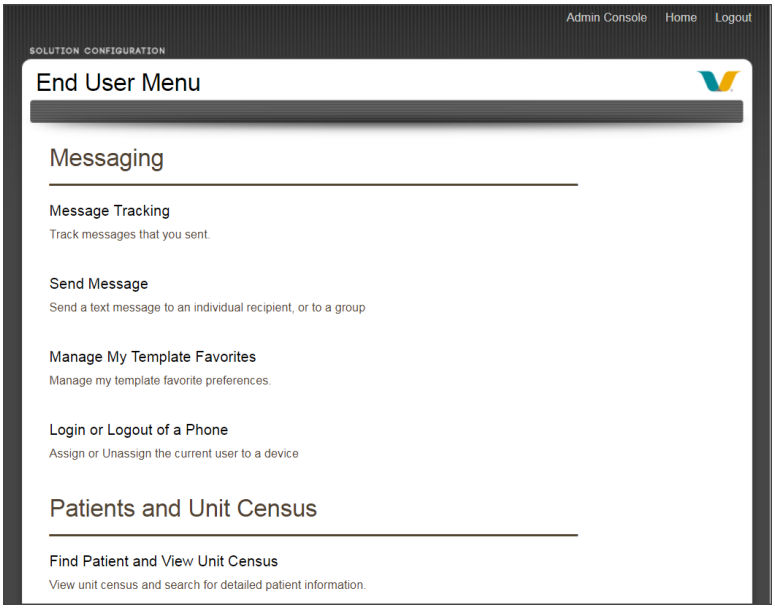
Execute a test to verify that the workflow functions as designed. When successful, the workflow test result displays in the Solution Configuration section.

To test a workflow that you created, follow these steps:

1. Select a workflow from the Workflows list. In this example, select the AdminMenu workflow.
   The AdminMenu workflow details display.
2. Select **Test** in the workflow menu.



   The workflow test is executed.
3. Verify the success or failure of the workflow test.
   In this example, the AdminMenu workflow test displays the Solution Configuration section.



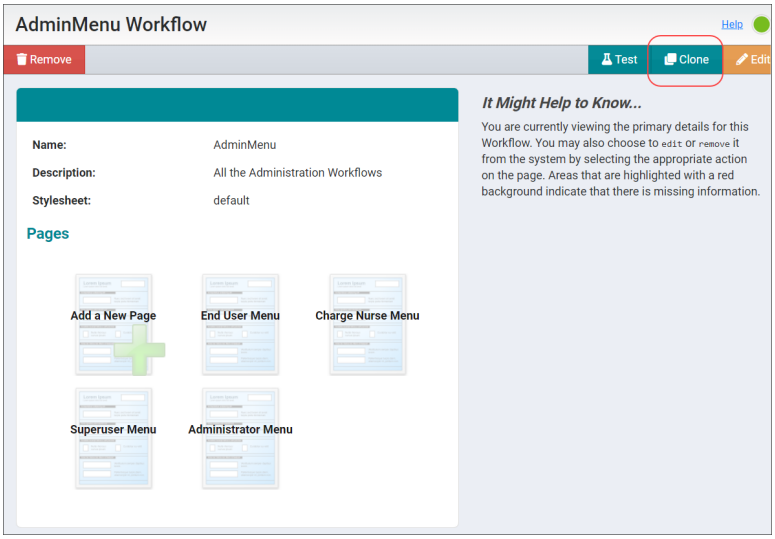
Cloning a Workflow

Use an existing workflow to create an identical copy that can then be edited to create a new workflow with similar characteristics.

Instead of creating an entirely new workflow, you can quickly modify the clone of an existing workflow. Using a clone as a template can save time and effort needed to create a workflow, depending on the amount of modification required to meet the specifications in the new workflow.

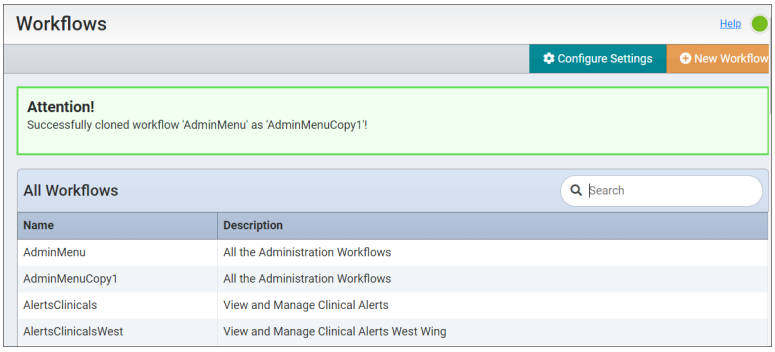
To clone a workflow, follow these steps:

1. Select a workflow from the Workflows list. In this example, select the AdminMenu workflow. The AdminMenu workflow details display.
2. Select **Clone** in the workflow menu.



   A success or failure message displays at the top of the Workflows page.
3. Verify the status of the clone creation process. In this example, the 'AdminMenuCopy1' workflow is created.

When successful, the new workflow appears in the list in alphabetical order. A new workflow is created with the same name as the original workflow, with 'Copy' and the number of the current copy appended.



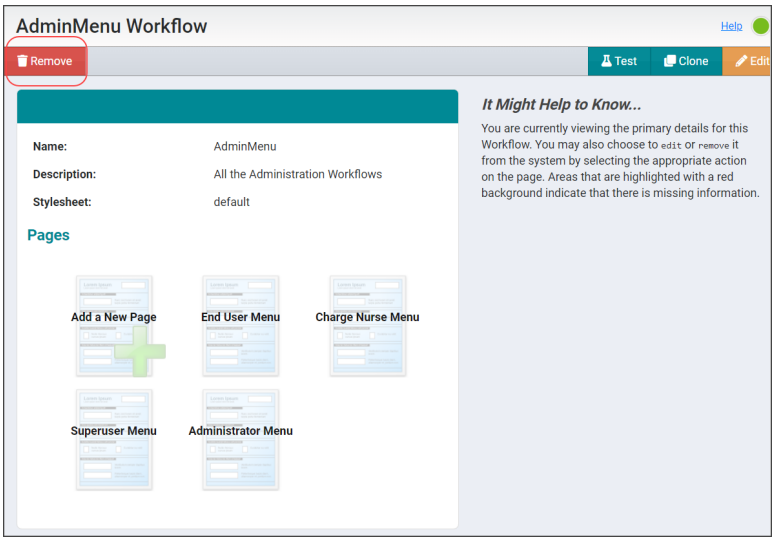
Rename the cloned workflow, and edit it to perform the needed functionality. See Editing a Workflow on page 313 for details.

Removing a Workflow

You can permanently remove a workflow from Vocera Platform.

Once removed, the workflow is no longer listed in the Workflows page. The workflow and related data cannot be retrieved.

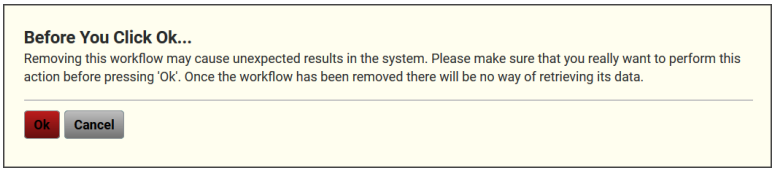
1. Select a workflow from the Workflows list. In this example, select the AdminMenu workflow. The AdminMenu workflow details display.
2. Select **Remove** in the workflow menu.



A system generated warning message appears.

3. Click **Ok** to proceed.

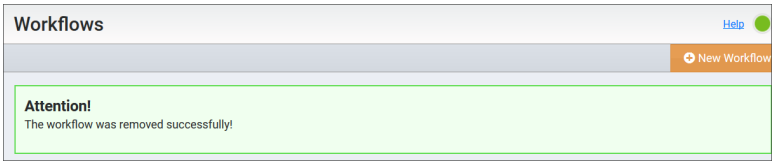
Warning: Removing this workflow may cause unexpected results in the system. Please make sure that you really want to perform this action before pressing 'Ok'. Once the workflow has been removed there will be no way of retrieving its data.



A success or failure message displays at the top of the Workflows page.

4. Verify the status of the workflow removal process.

   In this example, a success message displays at the top of the Workflows page. The removed workflow is no longer listed in Workflows.



Working With Workflow Pages

Create a new page, or view the configuration details of a selected workflow page and the options provided to manage the page. You can edit, remove, or clone the selected page.

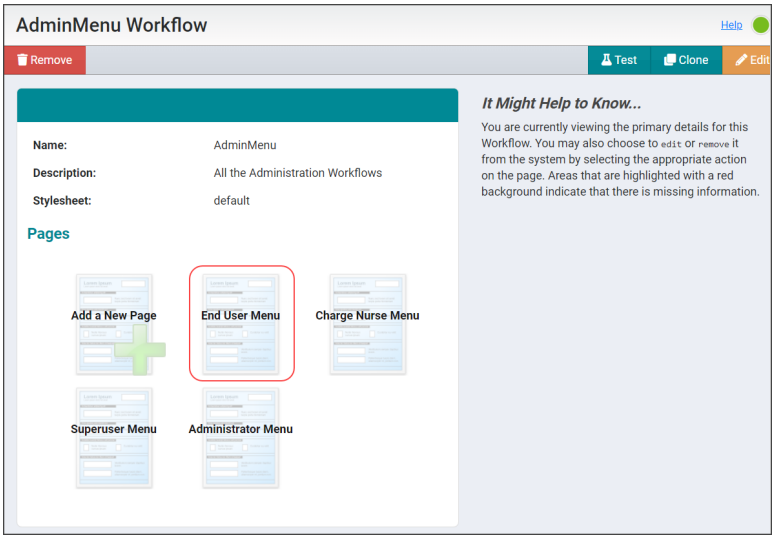
The configuration pages in the workflow's Pages section are icons; click an icon to edit the page. Drag and drop the page icons to organize the workflow's pages in this section.

The icon order is only useful for logical organization in this section, with the exception of the first page icon. The first page icon shown after the Add a New Page icon will present the page that is first accessed in the workflow. In this example, the content defined in the End User Menu page will appear first when a user's device receives data via the AdminMenu workflow.

1. Select a workflow from the Workflows list.

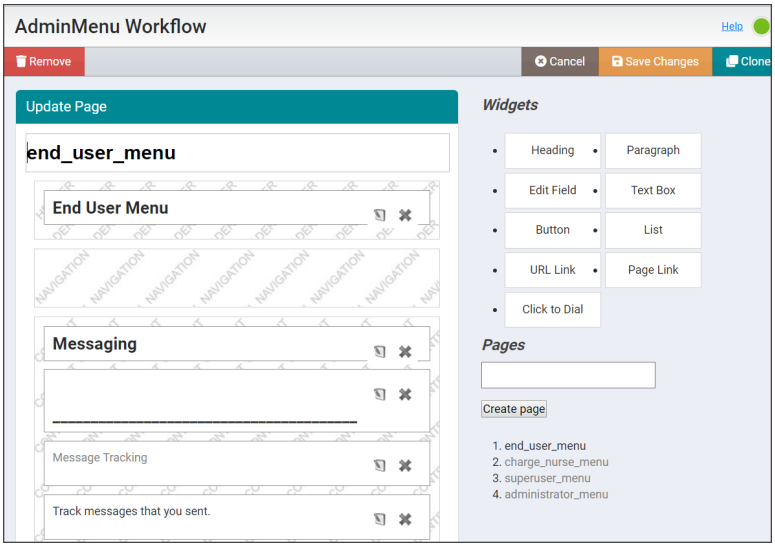
   The workflow's details display.

2. Select a workflow configuration page. In this example, select the End User Menu page.



The Update Page configuration options display for the selected workflow page.

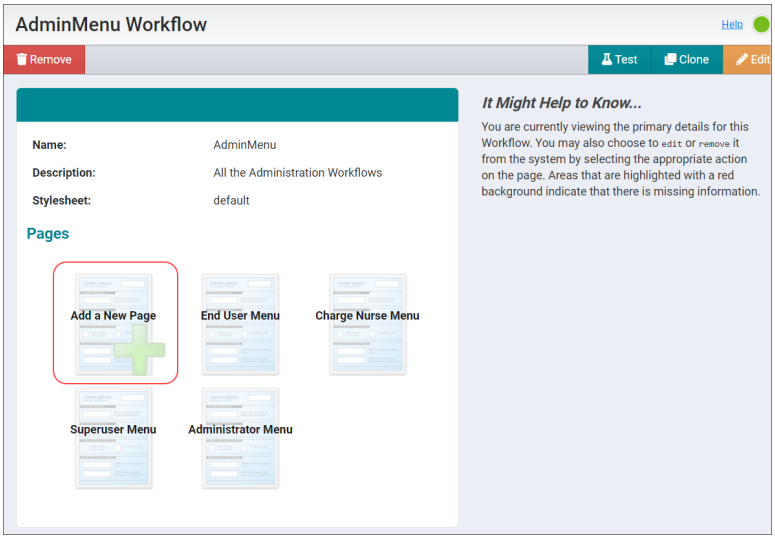
3. Manage the configuration details for the selected workflow page in the Update Page dialog as needed.



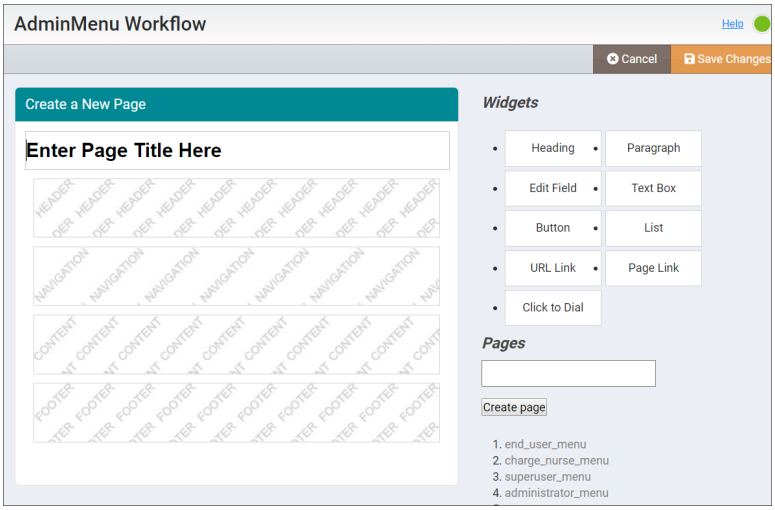
Creating a New Page

Create a new configuration page in an existing workflow.

1. Select a workflow from the Workflows list.
   The workflow's details display.
2. Select **Add a New Page** in the workflow's Pages section.



   The Create a New Page section displays.
3. Work with the provided widgets to configure the new page as needed.

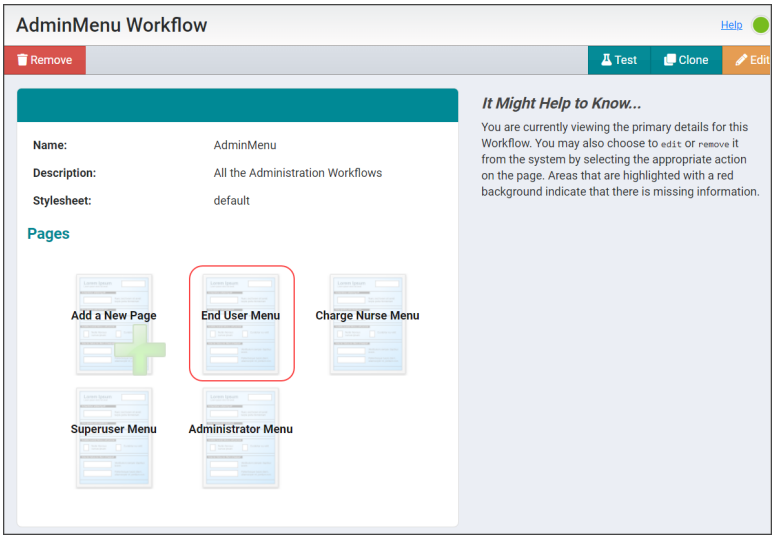


4. Select one of the following options to exit the configuration.
   - Select **Cancel** to return to the workflow's configuration section without adding a new page.
   - Select **Save Changes** to add the new page to the workflow's configuration section.

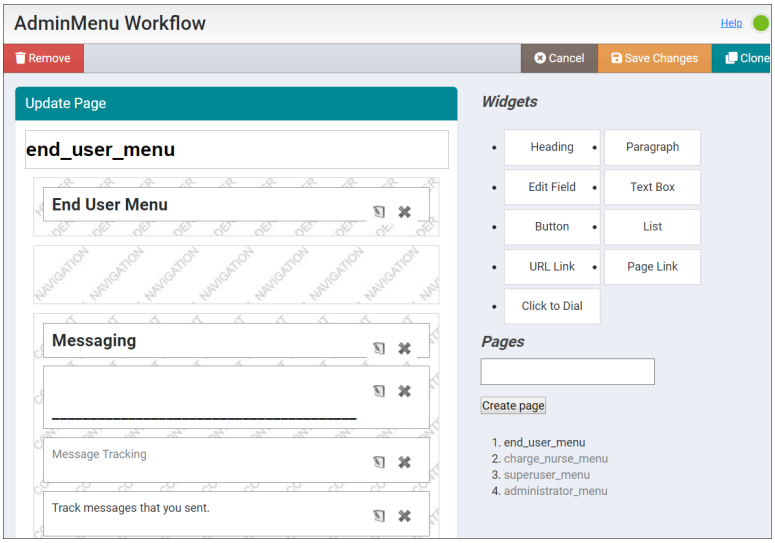
Editing a Page

Edit an existing configuration page in a workflow.

1. Select a workflow from the Workflows list.
   The workflow's details display.
2. Select a workflow configuration page. In this example, select the End User Menu page.



   The Update Page configuration options display for the selected workflow page.
3. Work with the widgets in Update Page to revise the page as needed.



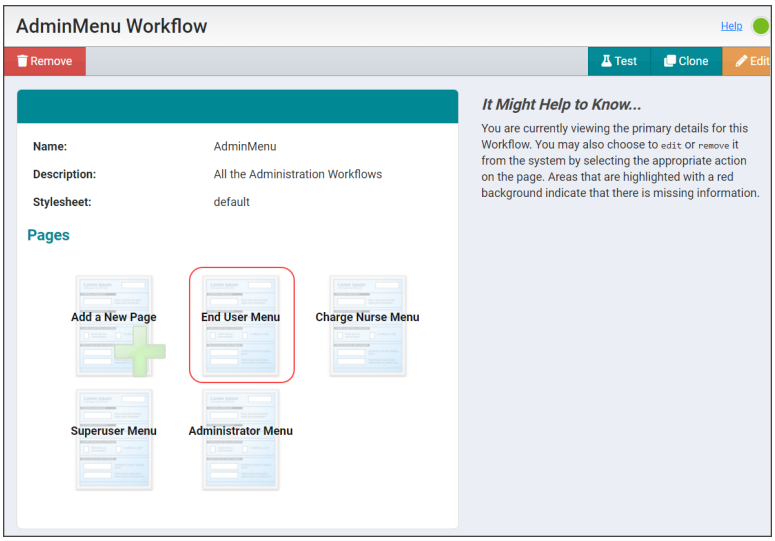
4. Select one of the following to exit the Update Page dialog.
   - Select **Remove** to delete the configuration page from the workflow. See Removing a Page on page 321 for details.
   - Select **Cancel** to return to the workflow view without making a change to the configuration page.
   - Select **Save Changes** to revise the configuration page.
   - Select **Clone** to make a copy of the configuration page. The copy can be edited to perform a similar function. See Cloning a Page on page 320 for details.

Cloning a Page

Use an existing workflow page to create a new workflow page that should have similar characteristics.

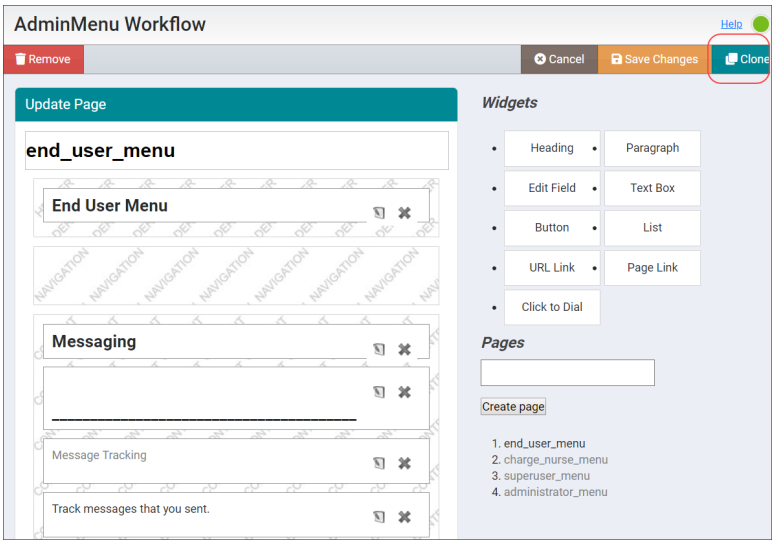
The new workflow page is created with the same name as the original workflow page, with 'Copy' and the number of the current copy appended. Once created, rename the cloned page and configure it to perform a needed function.

1. Select a workflow from the Workflows list.
   The workflow's details display.
2. Select a workflow configuration page. In this example, select the End User Menu page.



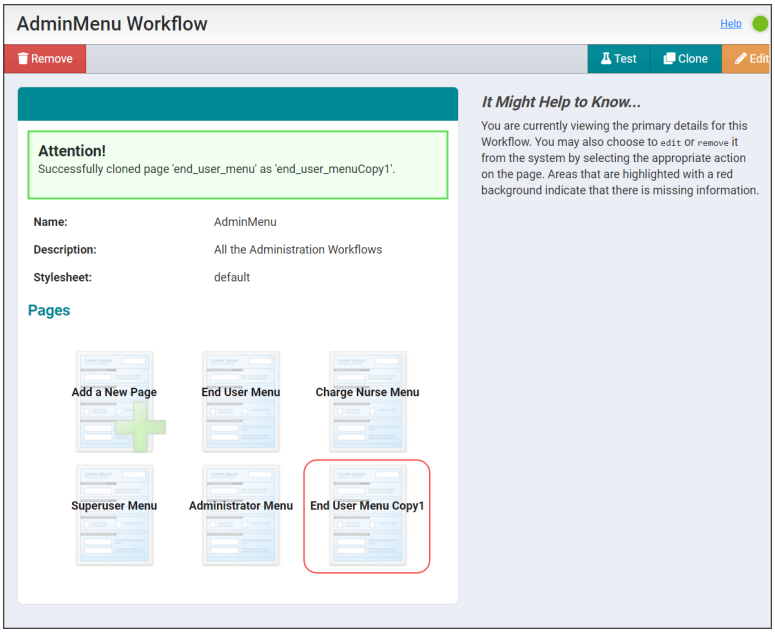
The Update Page configuration options display for the selected workflow page.

3. Select **Clone** in the configuration page.



A success or failure message displays at the top of the configuration section, and the new page displays in the Pages section.

4. Select the new page icon in the workflow's Pages section. The clone is displayed at the bottom of the list of page icons. In this example, select the End User Menu Copy1 page.



Rename the cloned page, and edit it to perform the needed functionality. See Editing a Page on page 319 for details.

Removing a Page

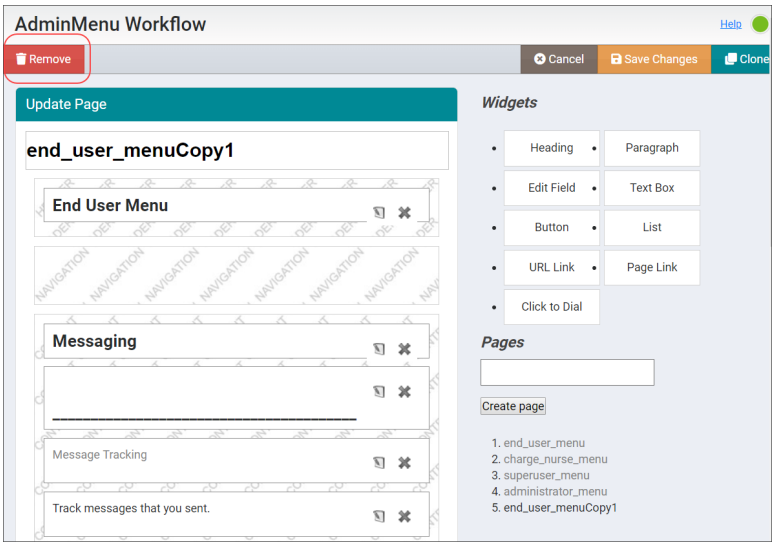
You can permanently remove a configuration page from an existing workflow.

Once removed, the workflow's configuration page is no longer available to the Vocera Platform, and you cannot retrieve the workflow page and related data.

To remove a workflow page, follow these steps:

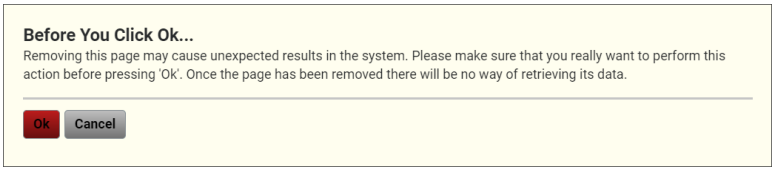
1. Select a workflow from the Workflows list. In this example, select the AdminMenu workflow.
   The workflow's details display.

2. Select a workflow configuration page. For example, select End User Menu Copy1 page to remove.
   The Update Page configuration options display for the selected workflow page.
3. Select **Remove** in the Update Page menu.



Warning: Removing this page may cause unexpected results in the system. Please make sure that you really want to perform this action before pressing "Ok". Once the page has been removed there will be no way of retrieving its data.

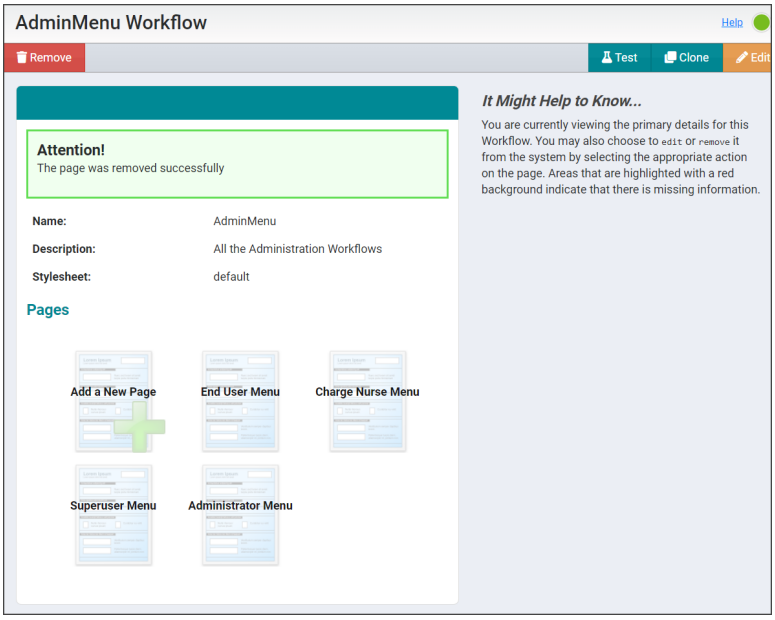
The following system generated warning message displays:



4. Click **Ok** to proceed with removing the page.

   A success or failure message displays at the top of the selected workflow's configuration section.
5. Verify if the page was removed.

   For example, if you removed the End User Menu Copy1 page successfully, the thumbnail icon for this page is no longer displayed in the Pages section as shown in the following screenshot.


AdminMenu Workflow
Help
Remove
Test
Clone
Edit
Attention!
The page was removed successfully
Name:
AdminMenu
Description:
All the Administration Workflows
Stylesheet:
default
Pages
Add a New Page
End User Menu
Charge Nurse Menu
Superuser Menu
Administrator Menu
It Might Help to Know...
You are currently viewing the primary details for this Workflow. You may also choose to edit or remove it from the system by selecting the appropriate action on the page. Areas that are highlighted with a red background indicate that there is missing information.

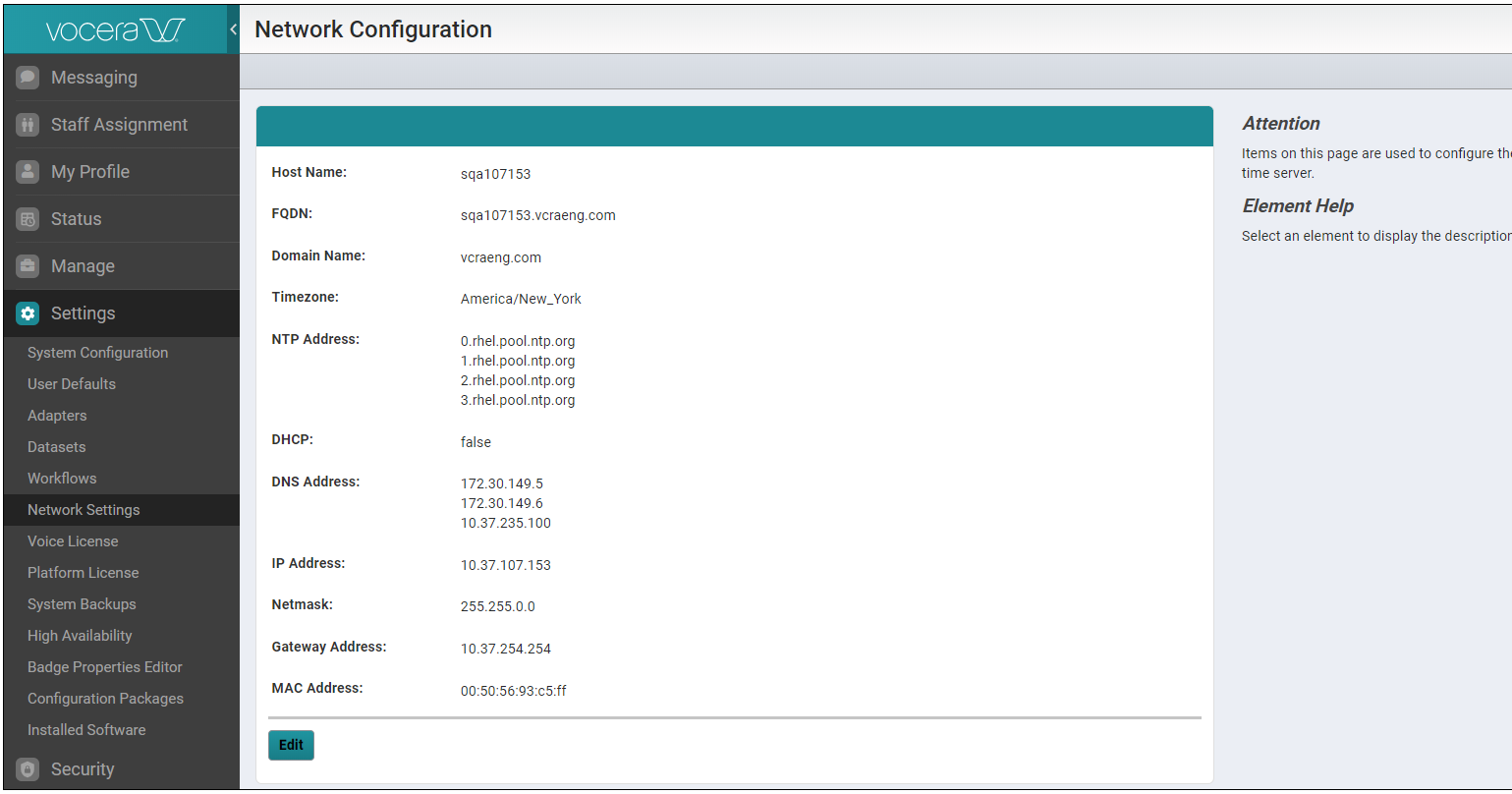
Network Settings

Configure TCP identity, time zone, and the time server settings for the network in the Vocera Platform.

A system administrator can access the **Network Settings** section before and after licensing the Vocera Platform.

In a High Availability (HA) environment, the system administrator configures the network requirements of a Vocera system before licensing it. You must uncheck the **DHCP** checkbox in the network settings when configuring an HA environment; the other network settings are configurable for any environment.

To view the network settings for your system, navigate to the **Settings** section of the Web Console, and select **Network Settings**. The Network Configuration page displays with information on network configuration fields.



Besides viewing the network configuration details of your system, you can edit the settings and update the configuration. To learn more about editing your network configuration, see Editing Network Settings on page 325,

Static or Dynamic IP Address Settings

Set network configuration settings for a dynamic or static IP address assignment.

Static IP Address Setting

A static IP address is required for the Vocera Platform to be a candidate for clustering. In the Network Configuration form fields, you must uncheck the **DHCP** checkbox to enable static IP address assignment. The network configuration fields must be populated with the required information to access the correct network.

We recommend that you do edit or modify the following fields before you set up Vocera Platformclustering in a high availability (HA) environment to prevent any undesirable system issues.

- Hostname
- Domain Name
- DHCP
- IP Address
- Netmask
- Gateway Address

To change the network configuration settings for static IP address assignment and learn about the field information, see Editing Network Settings on page 325.

Dynamic IP Address Setting

When the **DHCP** field is selected in the Network Configuration form, a standalone Vocera Platform is enabled to assign the IP address dynamically. The **IP address**, **Netmask**, and **Gateway Address** fields are disabled when the **DHCP** checkbox is selected.

The following configuration fields must be populated with the required information in order to access the correct network:

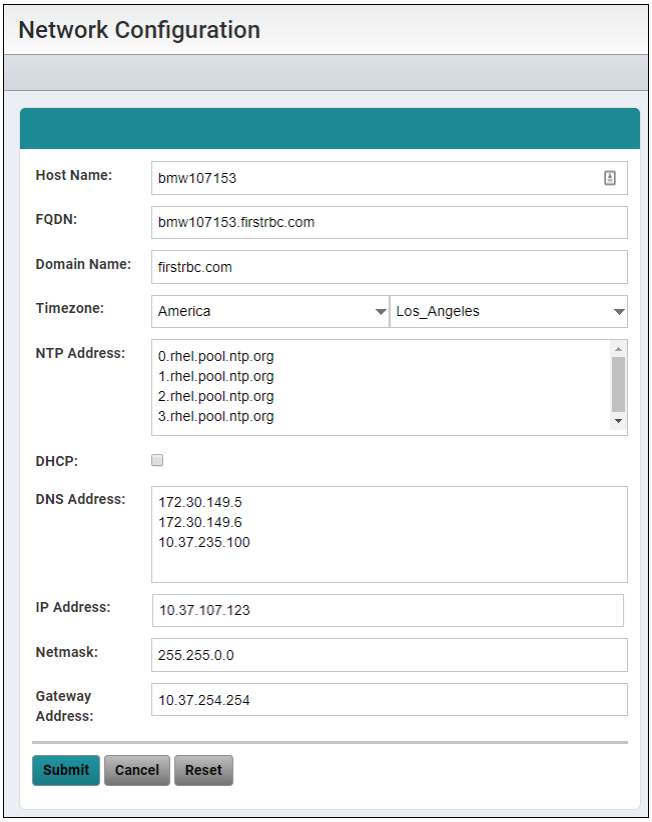
- Host Name
- FQDN
- Domain Name
- Timezone
- NTP Address
- DHCP
- DNS Address

To change the network configuration settings to enable dynamic IP address assignment and learn about the field information, see Editing Network Settings on page 325.

Editing Network Settings

Modify network settings and enter new values for network configuration fields.

1. Navigate to **Network Settings** in the **Settings** section of the navigation bar.
   The Network Configuration page displays.
2. Click Edit to display the editable fields for network configuration.



3. Edit the field information for the network configuration fields as desired.
   The following table describes the network configuration fields:

Network Configuration	Field Information
Host Name	Enter a name for the Vocera Platform used in the network; default value is Vocera.
FQDN	Enter a Fully Qualified Domain Name (FQDN) for the Vocera Platform.
Domain Name	Enter the name of the network domain used by the Vocera Platform.
Timezone	Enter the time zone in which the Vocera Platform operates.
NTP Address	Enter the values for Network Time Protocol (NTP) address to be used for calibrating time keeping.
DHCP	Specifies the Dynamic Host Configuration Protocol (DHCP). This option must be unchecked for the Vocera Platform to be in a high availability (HA) environment; the Vocera Platform is a candidate for clustering only if it has a static IP address. A standalone system can use dynamic or static addressing. To learn more about DHCP settings, see Static or Dynamic IP Address Settings on page 325
DNS Address	Address used to specify the Domain Name Server of the Vocera Platform.
IP Address	Enter the Internet Protocol (IP) address assigned to the Vocera Platform. The **IP Address** field is not configurable when DHCP is selected for a standalone system.

Network Configuration	Field Information
Netmask	Specifies the subnet and number of hosts reachable via layer 2 adjacency (Not Routed). The **Netmask** field is not configurable when DHCP is selected for a standalone system. .
Gateway Address	Enter the address that allows routable access outside the private network. The **Gateway Address** field is not configurable when DHCP is selected for a standalone system.
MAC Address	Enter the Media Access Control (MAC) address used as a unique identifier for communications. The **MAC Address** field is populated automatically.

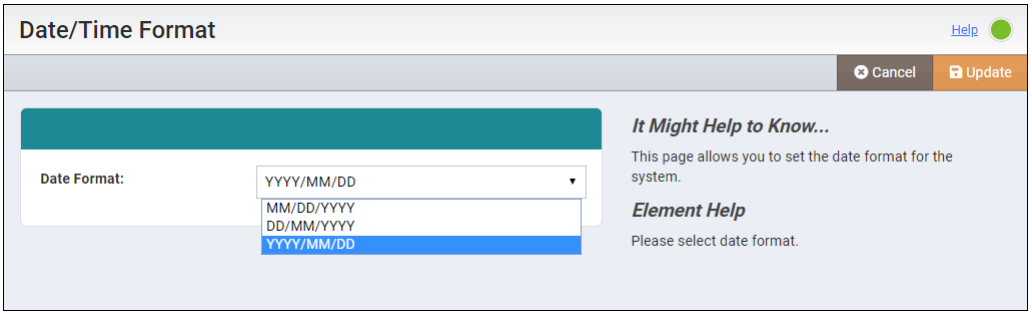
4. Select one of the following to exit the network configuration form:
   - **Submit** — to save changes to the network configuration fields and exit the form.
   - **Reset** — to undo any recent changes to the network configuration fields.
   - **Cancel** — to exit the network configuration form without saving any changes.

Selecting a Date and Time Format

Select a preferred date and time format for the system.

System administrators for facilities outside of the United States (non-US locales) can select a preferred date and time format to support the local date and time formats.

1. Navigate to **Network Settings** in the **Settings** section of the navigation bar.
   The Network Configuration page displays.
2. Click **Date/Time Format**
   The Date/Time Format page displays.
3. Select a value for Date Format field from the dropdown list



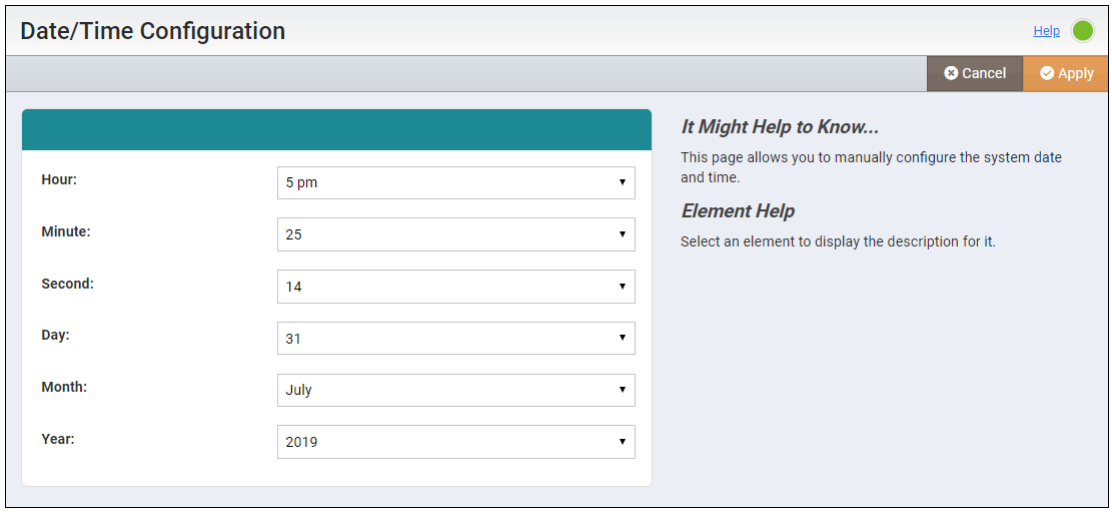
   The "DD/MM/YYYY" is the default format for US locales.
4. Select one of the following to exit the Date/Time format page:
   - **Update** — to save the selected Date/Time format and return to the Network Configuration page.
   - **Cancel** — to exit the Date/Time Format page without saving any changes.

Configuring System Date and Time

Manually configure the system level date and time values.

The network time protocol (NTP) address field in the **Network Settings** section automatically sets the system's clock. In the event that the clock is wrong and NTP is unable to correct it, you can use the **Date/Time Configuration** to correct the clock.

1. Navigate to **Network Settings** in the **Settings** section of the navigation bar.
   The Network Configuration page displays.
2. Click **Date/Time Configuration** on the right hand corner.
   The Date/Time Configuration page displays.



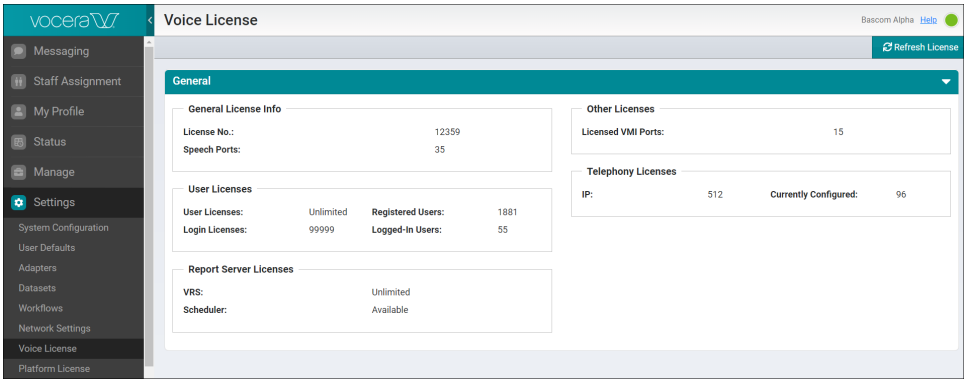
3. Click on the dropdown arrow next to a field to display a list of available values.
4. Select a value for the Hour, Minute, Second, Day, Month, and Year fields as needed.
5. Select one of the following to exit the Date/Time Configuration page:
   - **Apply** — to save the selected values and return to the Network Configuration page.
   - **Cancel** — to exit the Date/Time Configuration page without saving any changes.

Voice License

The **Voice License** page displays information about the features supported by the Voice license that your system is using as well as thresholds for supported features, such as the number of concurrent users you are allowed or the number of telephony ports available to your system. The information on this page is display only; it reflects the capabilities provided by your underlying license. If you have updated your license at the command line and the Vocera Platform Web Console does not display your new capabilities, you may also use this page to refresh the display of your license information.

To display or refresh Voice license information:

1. Navigate to **Voice License** in the **Settings** section.
   The **Voice License** page appears.



2. Review the information on this page to confirm the capabilities of your Voice license.
   The **General License Info** section displays the following:

Field	Description
License Number	The segment of the license key that uniquely identifies your organization.
Speech Ports	Specifies the number of ports available for speech recognition. Each active Genie session decrements the number of available ports by one. That port becomes available again when the Genie session ends (that is, when the speech recognition is complete or when the user the user cancels the Genie interaction), so a speech port is typically busy for only a few seconds at a time.

   The **User Licenses** section displays the following:

Field	Description
User Licenses	The number of user profiles you may create in your system. An Enterprise license provides unlimited **User Licenses** and a limited number of **Login Licenses**.
Login Licenses	The number of users who may log into devices concurrently.

Field	Description
Registered Users	The number of actual user profiles currently in your system. You can determine the number of user profiles still available by subtracting the number of **Registered Users** from the number of **User Licenses**.
Logged-In Users	The number of users who are currently logged into devices. You can determine the number of concurrent logins still available by subtracting the number of **Logged-In Users** from the number of **Login Licenses**.

The **Report Server Licenses** section displays the following:

Field	Description
VRS	Displays the type of Vocera Report Server license provisioned for your system (Not Available, Basic, or Unlimited).
Scheduler	Specifies whether the Report Scheduler feature is provisioned for your system.

The **Other Licenses** section displays the following:

Field	Description
Licensed VMI Ports	Displays the number of VMI (Vocera Messaging Interface) ports provisioned for your system. Each VMI integration consumes a single port.

The **Telephony Licenses** section displays the following:

Field	Description
IP	The number of telephony lines provisioned for your system. The Vocera Platform supports either an IP PBX or a VOIP gateway.
Currently Configured	The number of telephony lines currently configured for use by your system. You can determine the number of telephony lines still available by subtracting the number of lines in the **IP** field from the number of lines in the **Currently Configured** field.

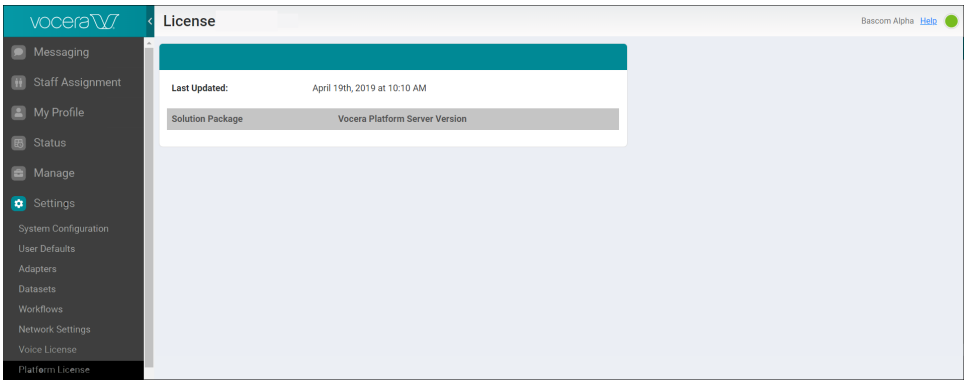
3. If you need to refresh the page to view the capabilities of a new license, click **Refresh License** in the top-right area of the page.
   The screen refreshes and displays the new license capabilities.

Platform License

The **Platform License** page displays the last time the license file was updated and also the names of any solution packages that were imported as part of the licensing process.

To display Platform license information:

1. Navigate to **Platform License** in the **Settings** section.
   The **License** page appears.



2. Review the information on this page to confirm the solution packages you have imported.

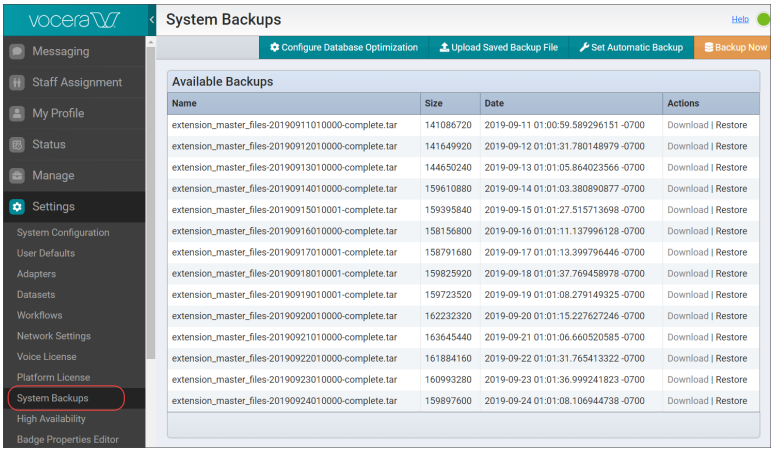
System Backups

You can create and manage backup files of the entire system, including stored data and configured adapters.

Regular backups are an important practice for any system storing critical information. Backups provide insurance against loss of information and configuration.

Backup files are snapshots of the Vocera Platform at the time of the system backup. A backup file includes all adapter and solution configuration files, as well as the voice and other data stored in the Vocera Platform.

Backup files are managed through the **System Backups** section in the Vocera Platform Web Console.



The complete system backup is a single TAR file that includes the system databases. You can restore a single backup to get the system back online after performing maintenance or a disaster recovery. All files needed for system restoration should be included in the daily backup snapshot.

Note: Backups can only be taken when the system is not in the MAINTENANCE Node State.

When you are logged into the private IP address of a system associated with a high availability cluster, you cannot access System Backups.

Each system backup is stored on the Vocera Platform with the date and time of the backup. If a backup file is restored immediately after it is created, there are no functional changes to the system.

Note: The system backup should be treated as if it contains protected health information (PHI).

Vocera recommends keeping the system backup files in a secure location to protect data. The Vocera Platform Web Console provides the ability to export a backup to an external location for safe keeping. Adding password protection to the backup file is also recommended.

In System Backups you can perform a manual backup, or configure automatic backups. You can configure the system to automatically store backup files in a secure location, on a selected schedule. Once a backup file is created, you can perform the following tasks:

- Download the backup file for storage
- Upload a saved backup file to the system
- Restore a current backup file

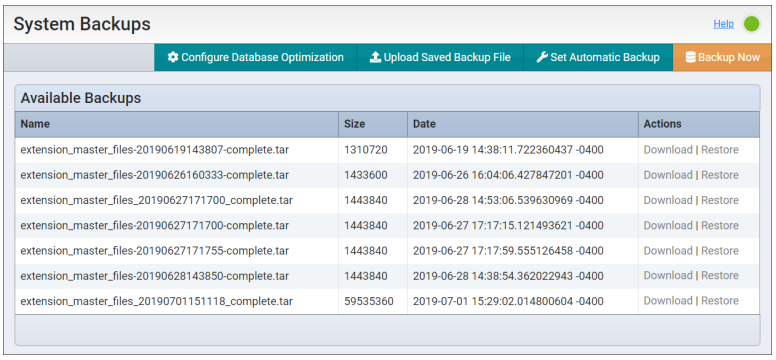
The System Backup functionality also allows you to configure the default database optimization settings in order to reclaim storage. A vacuum process is performed periodically to optimize the database, especially on frequently-updated tables in the database. For more information, refer to Understanding Database Optimization on page 334.

Accessing the System Backups List

A list of the system backups retained on your Vocera system displays in the Available Backups table.

The latest backup file displays at the bottom of the list. When the number of backup files exceeds the configured maximum limit for your installation, the oldest file is deleted.

1. Navigate to **System Backups** in the **Settings** section of the Vocera Platform Web Console.
   The System Backups page appears.



2. Review the **Available Backups** table to understand the fields displayed in the backups list.

Field	Description
Name	Displays the system generated name of the created backup file. The backup files are .tar, .tar.gz, or .backup file types.
Size	Displays the size of the created backup file.
Date	Displays the date on which the backup file was created as a system generated datetime.
Actions	Select an option to download or restore the specified backup file, as needed. Select **Download** to save the backup file for storage. Select **Restore** to overwrite the current backup with the selected backup.

What to do next: Use one of the options in this page to configure database optimizaton, upload a saved file, set an automatic backup, restore a backup, or perform a manual backup. For instructions, refer to the System Backups on page 332 documentation.

Understanding Database Optimization

A daily process physically removes unused data from the database on a configurable schedule.

In normal PostgreSQL operation, a tuple (sequence of terms) that is deleted or obsoleted by an update is not physically removed from the table; storage space is occupied by "dead" tuples until a 'VACUUM' procedure is performed. A vacuum procedure should be performed periodically to optimize the database, especially on frequently-updated tables in the database.

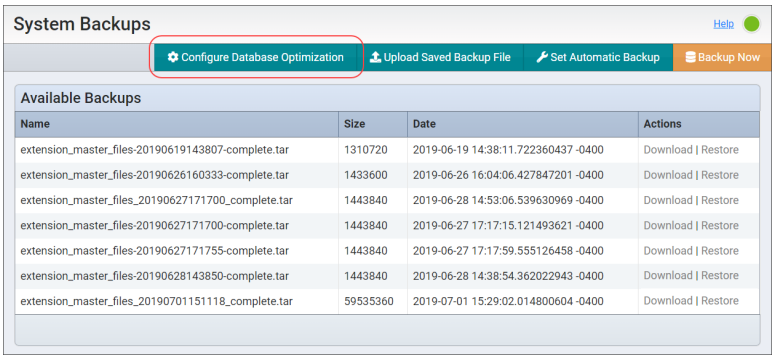
Facility optimization needs vary, depending on database usage. By default in the Vocera Platform, a vacuum procedure is performed daily to optimize database performance. You can configure the date and time for the daily scheduled optimization, or change to a weekly schedule, in the Vocera Platform Web Console.

Configuring a Database Optimization Schedule

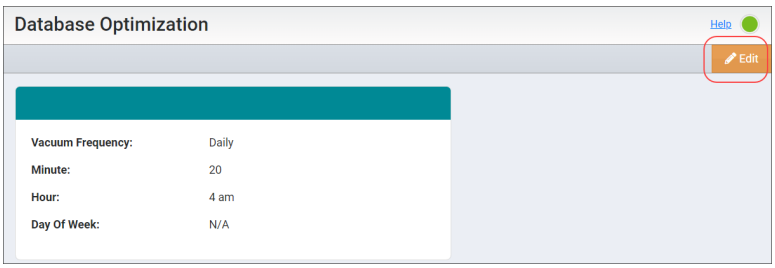
Configure a vacuuming schedule to optimize the Vocera system's database performance.

By default, database vacuuming is scheduled to occur at 4:20 a.m. daily. You can select a daily or weekly optimization schedule, and configure the hour and minute settings.

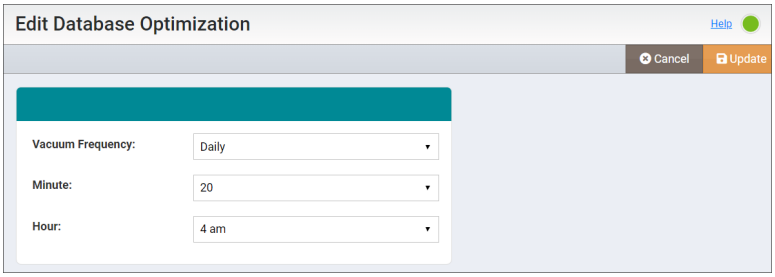
1. Navigate to **System Backups** in the **Settings** page of the Vocera Platform Web Console.
   The System Backups page appears.
2. Select **Configure Database Optimization** in the System Backups page.



   The Database Optimization page displays.
3. Click **Edit** in the Database Optimization page.



   The Edit Database Optimization dialog displays.

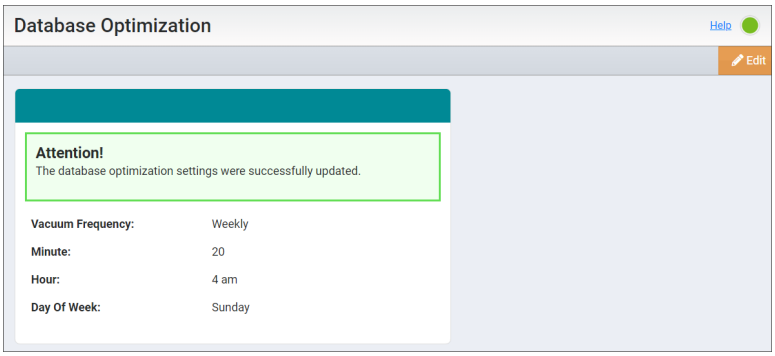


4. Define the settings for a database optimization schedule in the **Edit Database Optimization** dialog.

Parameter	Description
Vacuum Frequency	Select an option from the dropdown list to perform the optimization daily or weekly. The default selection is Daily. When weekly vacuuming is selected, the **Day of Week** field displays.
Day of Week	Use the arrow to select the day of the week for the vacuuming to occur. When weekly vacuuming is selected in the **Vacuum Frequency** field, this Day of Week field displays.
Minute	Select the minute from the dropdown list for the vacuuming to occur, if desired.
Hour	Select the hour from the dropdown list for the vacuuming to occur.

5. Select an option to exit the Edit Database Optimization dialog:
   - Select **Update** to save your changes and implement the new schedule.
   - Select **Cancel** to exit the page without changing the current optimization schedule.

   A success or failure message displays when **Update** is selected. This example displays a successful schedule update message.



Understanding Manual System Backups

Manually make a copy of the Vocera system as it is configured at the time of the system backup.

You can perform a manual backup at any time. After performing a manual backup, the latest backup file appears at the bottom of the Available Backups list.

When the number of backups exceeds the configured maximum limit for your installation, the oldest file is deleted. See Configuring the Automatic Backup General Settings on page 344 for information about enabling daily backups and configuring backup retention.

Create a system backup before restoring an earlier captured backup, or initiating any upgrades or installations that might impact the Vocera system.

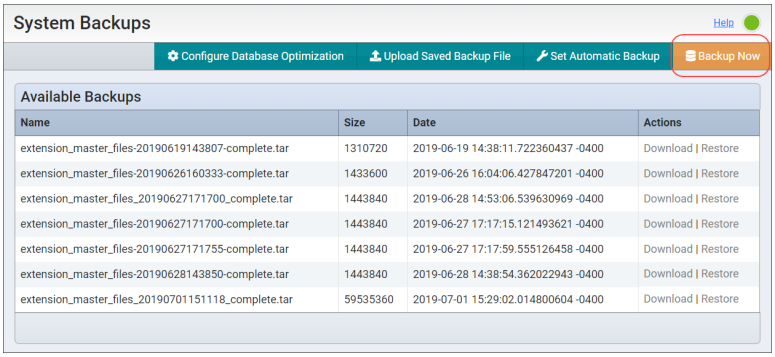
Important: Make a manual backup just prior to restoring a saved backup; restoring a backup is an irreversible action.

Creating a Manual Backup

Create a manual backup of the system and access the backup file in Available Backups.

The latest backup file displays at the top and the oldest backup file is displayed at the bottom of the Available Backups list.

1. Navigate to **System Backups** in the **Settings** page of the Vocera Platform Web Console. The System Backups page appears.
2. Select **Backup Now** in the System Backups page.



   A success or failure message displays, and the list of available backup files is refreshed.
3. Access the new backup file at the top of the Available Backups list.

Next, download the system backup file for secure storage. See Downloading a System Backup on page 337 for details.

Understanding a System Backup Restore

When necessary, any available backup file may be used to restore the system to a previous state.

To use a saved backup file to restore the system, the backup file must be located on the Vocera Platform. Backup files stored externally must be uploaded to the Vocera system for restoration.

Note: The upload process automatically invokes the restore process; refer to Uploading a Saved Backup File for details.

You can restore a saved backup file when it displays in the System Backups list in the Vocera Platform Web Console. Choose a backup file from the list to overwrite the current system with the previously stored backup file as described in Restoring a System Backup on page 338. The restoration process may take some time depending on the size of the database. Any data changed while the restoration is in progress will not be transferred to the new database.

Warning: Restoring a backup overwrites the existing information on the Vocera Platform. This action cannot be undone, and any information lost cannot be recovered.

After a backup is restored, database migrations are performed to ensure that the database is usable. For example, you may restore an older backup and find that the current XMPP adapter now requires a new attribute that is not present in the old backup.

Review the following key details for restoring system backup files:

- The restore operation recognizes legacy production database backups (.backup) and allows them to be restored.
- The restore operation recognizes gzipped backups (.tar.gz) and allows compatible items to be restored.
- During the restore process any differences in software or bundle versions, between the current system and the system on which the backup was created, are automatically displayed. A message displays when there are any differences between software versions; this message contains a View Differences link to review the version details.
- The mirth checkbox is disabled if the backup does not contain a mirth backup.
- The audit checkbox is disabled if the audit database is not restorable.
- The automatic backup timers checkbox is disabled if the backup does not contain systemd timers.

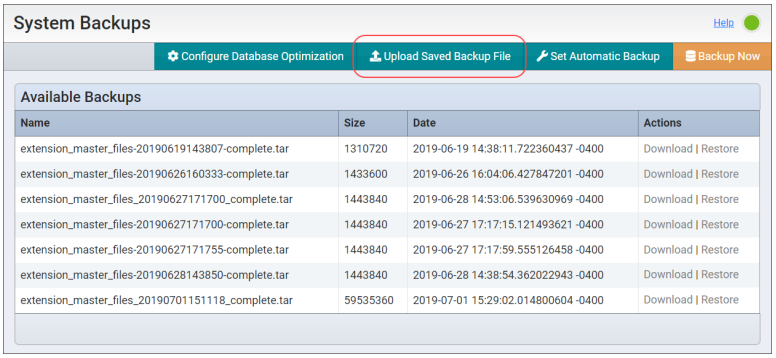
- Backups can only be restored when the Vocera Platform is in standalone mode.
- Adapters may only be disabled upon restore if the system database is being restored.

Uploading a Saved Backup

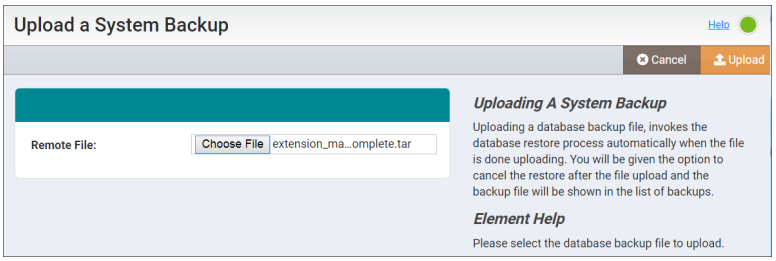
A system backup file that has been saved in a secure storage location can be uploaded and accessed in the Vocera Platform Web Console.

Uploading a backup file automatically invokes the restore process when the upload is complete. When the **Restore Options** dialog appears, select **Cancel** to display the System Backups page and access the uploaded file.

1. Navigate to **System Backups** in the **Settings** page of the Vocera Platform Web Console.
   The System Backups page appears.
2. Select **Upload Saved Backup File** in the System Backups page.



   The Upload a System Backup dialog displays.
3. Click **Choose File** in the **Remote File** field to locate the file to upload to the Vocera system.



4. Select one of the following to exit the **Upload a System Backup** dialog.
   - Select **Upload** to save the file to the Vocera Platform.
   - Select **Cancel** to close the dialog without making changes.

   It may take a significant amount of time for an upload to complete.
5. Review any compatability issues that are automatically discovered in the upload process.
   A compatibility check runs in the background to search for package and bundle differences on the system. Refer to Viewing Compatibility Issues on page 340 for additional information.

What to do next: When the upload is complete, the **Restore Options** dialog appears. Refer to Restoring a System Backup on page 338 for instructions on restoring system backups.

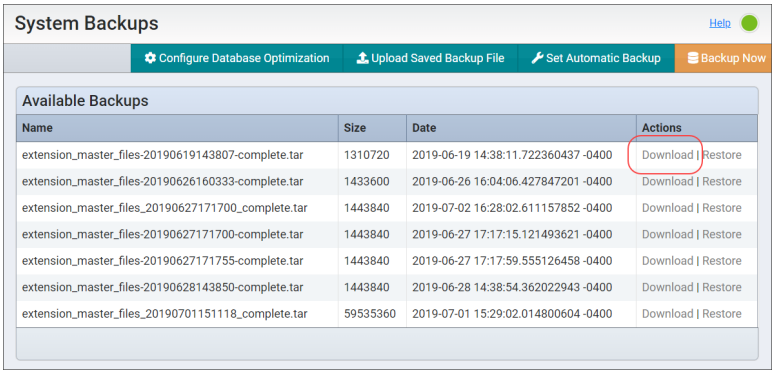
Warning: Restoring a backup overwrites the existing information on the Vocera Platform. This action cannot be undone, and any information lost cannot be recovered.

Downloading a System Backup

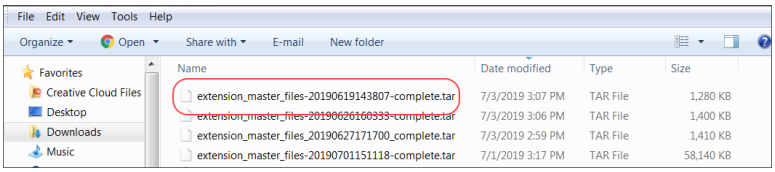
Download a system backup file to the Vocera system for access.

You can download a copy of a backup file to the Vocera system in order to transfer the file to secure storage. See your System Administrator for assistance with designated storage locations.

1. Navigate to **System Backups** in the **Settings** page of the Vocera Platform Web Console.
   The System Backups page appears.
2. Locate the system backup file that you wish to download in the **Available Backups** list.
3. Select **Download** in the Actions column.



   A copy of the file is downloaded to the system's configured download location.
4. Locate the system backup file. In this example, the file is saved in the Downloads folder on the Vocera appliance.



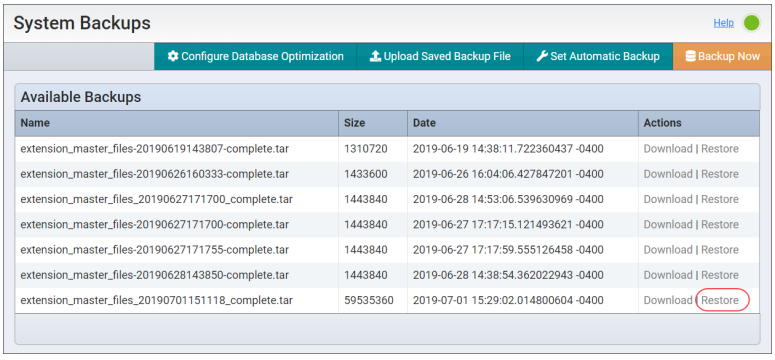
5. Manage the downloaded backup file as desired. For example, you may wish to transfer the system backup file to your designated storage location.

Restoring a System Backup

Restore a system backup file to be the current active system on the Vocera Platform.

In the restore process, first a compatability check is performed in the background, then you can make your component selections for the restore backup, and finally apply the backup file to the system. Once the restore is complete, you are presented with the login screen to access the Vocera Platform Web Console.

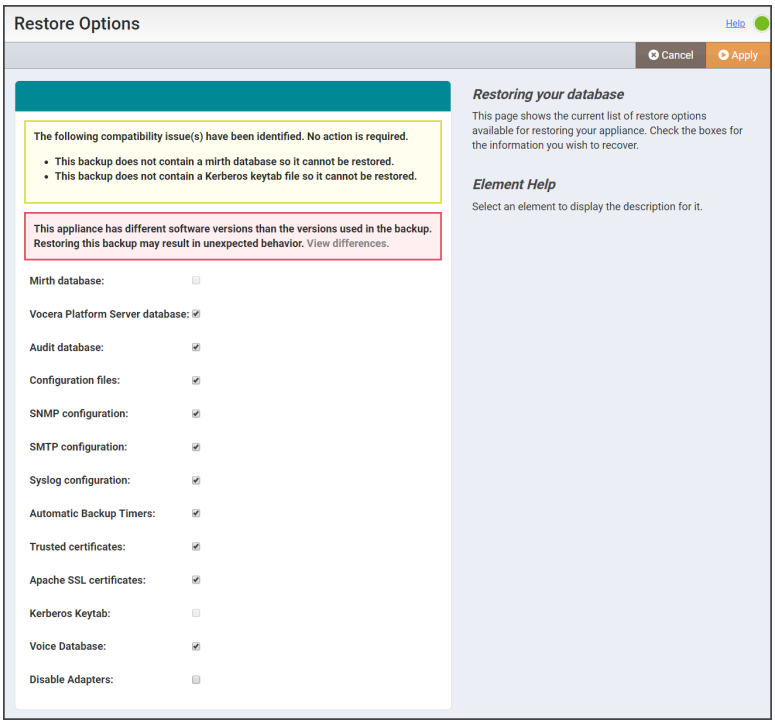
1. Navigate to **System Backups** in the **Settings** page.
   The System Backups page displays.
2. Select **Restore** in the Actions column for the selected system backup file in the System Backups page.



A compatibility check runs in the background to identify package and bundle differences on the system, then the Restore Options dialog displays.

3. Review the messages that display at the top of the **Restore Options** dialog when the compatibility check identifies software differences between systems. Refer to Viewing Compatibility Issues on page 340 for additional information.

   By default, all checkboxes are selected for a backup.

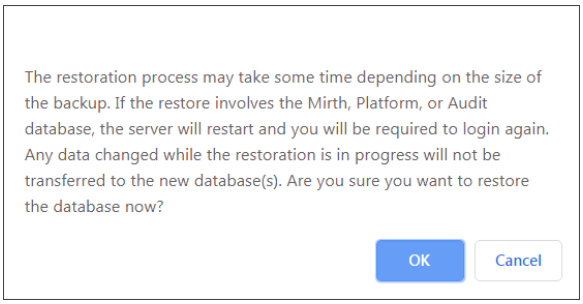


4. Select one of the following options to exit the **Restore Options** dialog.
   - Select **Apply** to overwrite the current system with the uploaded system backup.
   - Select **Cancel** to return to the System Backups page without making a change.

   A message dialog displays when Apply is selected.

5. Select one of the following options to exit the message dialog.

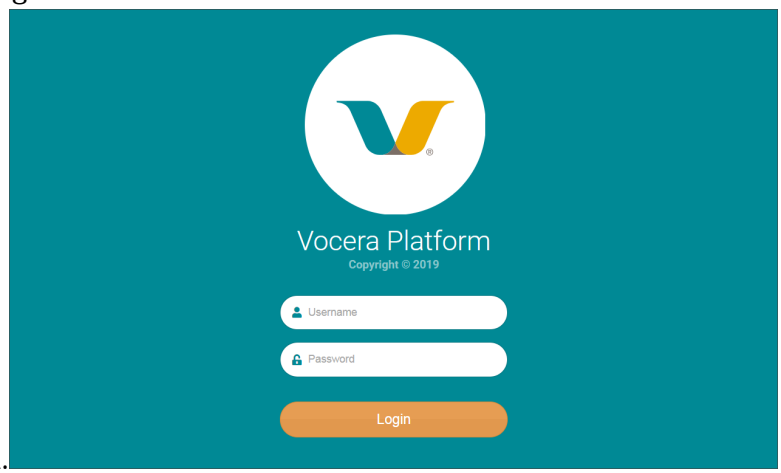
Warning: Restoring a backup overwrites the existing information on the Vocera Platform. This action cannot be undone, and any information lost cannot be recovered.



   - Select **OK** to accept the warning and proceed with the restoration.
   - Select **Cancel** to close the warning message without making changes.

   The restore process may take some time and will display a spinning wheel to indicate the action is still in process. When complete, the Vocera Platform Web Console login page appears.

Next, log into the Vocera Platform Web Console to access the restored system.



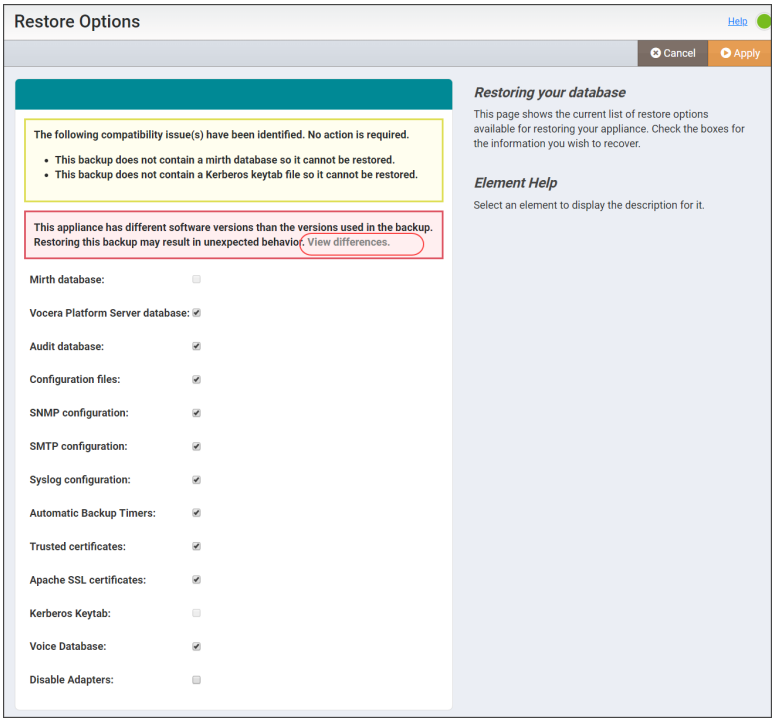
Viewing Compatibility Issues

When restoring a backup file, you can view a comparison between the system backup file you wish to restore, and the current system, which will be overwritten by the restore file.

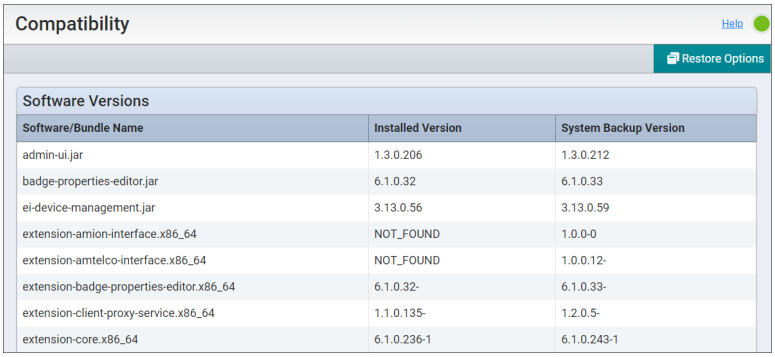
In the process of restoring a system backup, a compatibility check automatically runs in the background to check for package and bundle differences on the current system. A Compatibility page is displayed when differences are found.

Note: Uploading a system backup file automatically invokes the restore process when the upload process is complete. Refer to Uploading a Saved Backup on page 337 for details.

1. Restore a selected backup file on the Vocera system. Refer to Restoring a System Backup on page 338 for details.
   The Restore Options page displays.
2. Click **View Differences** in the message that displays in the Restore Options page.



   The Compatibility page displays.



3. Review the details displayed in the **Software Versions** table. This table provides a view-only table of the software names and versions for informational purposes.

Field	Description
Software/Bundle Name	Provides the name of the software or bundle file.
Installed Version	Identifies the version number of the file which is currently installed on the system.
System Backup Version	Identifies the version number of the file selected in the Restore procedure to replace the current system.

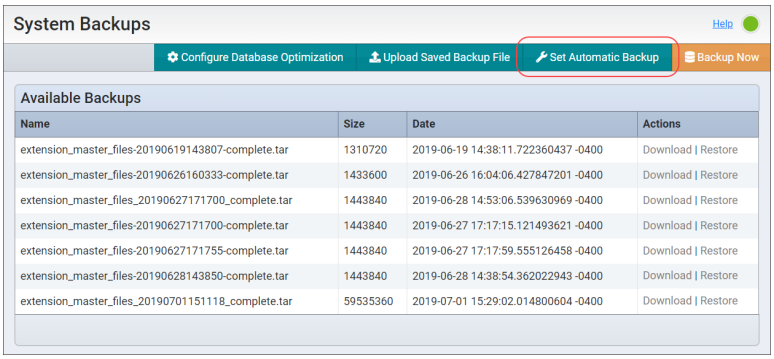
4. Click **Restore Options** to exit the Compatability page.
   The Restore Options page displays.

Next, choose to apply the backup file to the Vocera system, or to cancel the restore without changing the system. Refer to Restoring a System Backup on page 338 for details.

Understanding the Automatic Backups

Automatic backups allow you to automatically backup specified Vocera system information to a specified external location on a desired schedule.

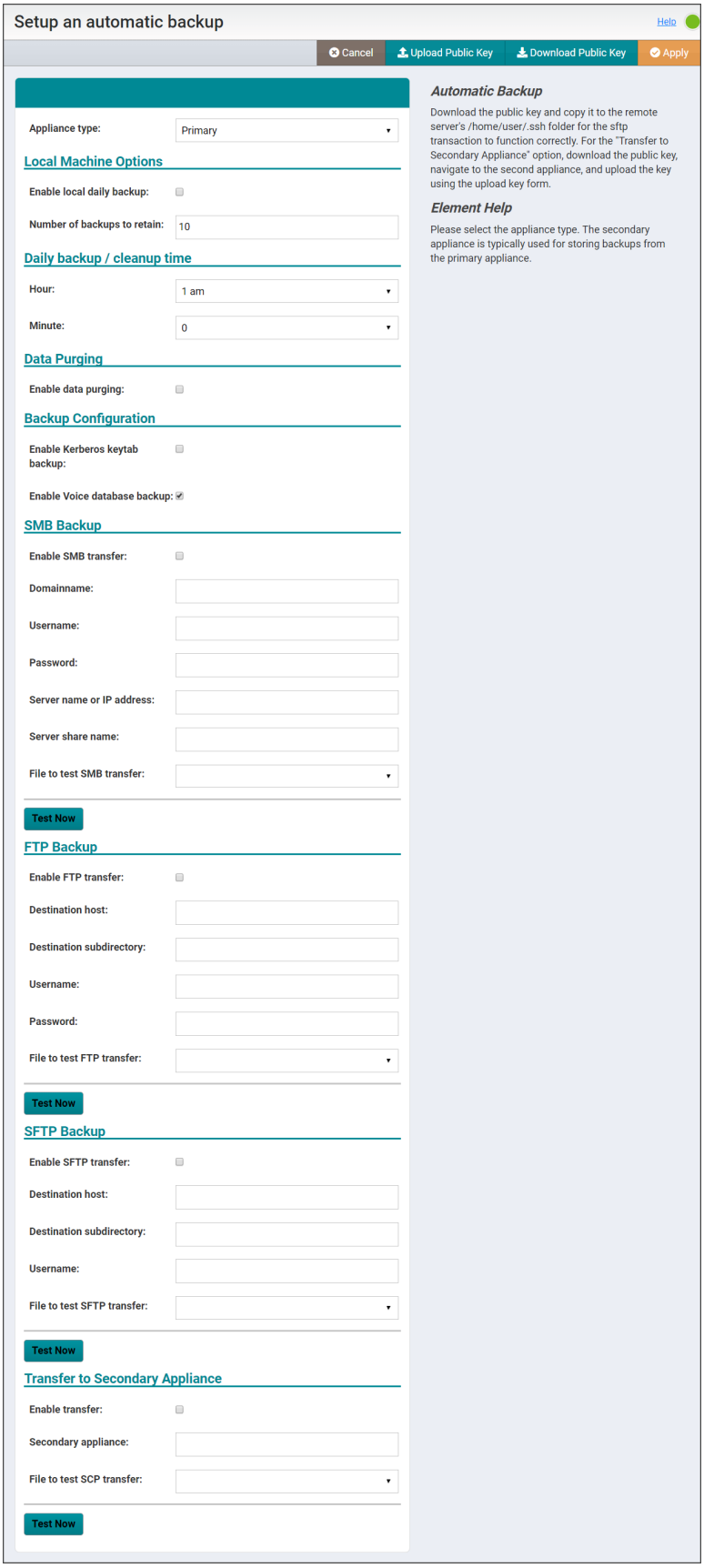
You must perform manual backups until an automatic backup is configured for the system. Automatic backups can be configured in **System Backups** in the Vocera Platform Web Console.



Automatic backups of the Vocera Platform can be configured to transfer backup files daily to an external location, such as a central information storage system, at a specified time. The Automatic Backups functionality allows you to configure the following transfer methods for backup files; SMB, FTP, SFTP, and transfer to a secondary Vocera appliance. When an external location is configured for backups, the backup files are automatically transferred to the specified IP address or server location for storage.

Once the automatic backup is configured, you can perform a test transfer to ensure that the configuration is accurate. Using a backup file from the current list of available backups, this test will verify that the backup files are transferred successfully.

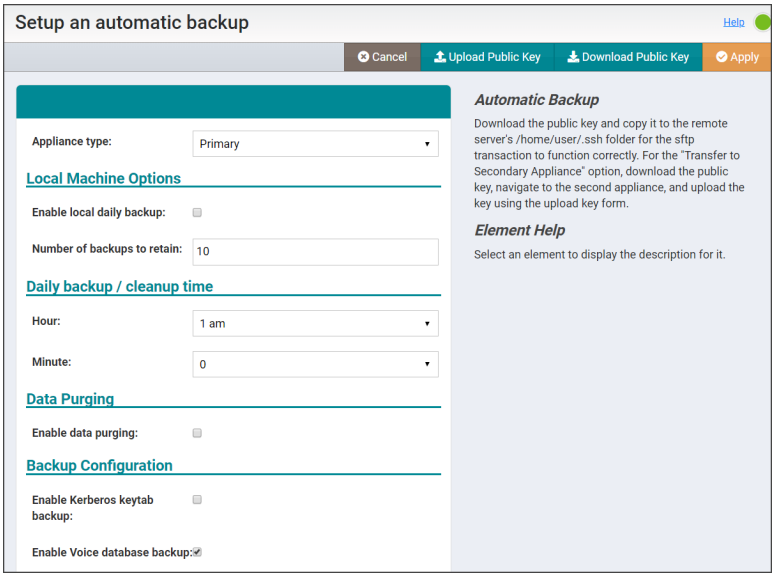
As shown in the **Setup an automatic backup** page, you can specify local machine or system backup options, in addition to managing the automatic backup storage options. The Vocera system configurations include the option to enable local machine, Kerberos keytab file, and Voice database backups. In addition you can configure a database optimization schedule and enable data purging.


Setup an automatic backup
Help
Cancel
Upload Public Key
Download Public Key
Apply
Appliance type:
Primary
Local Machine Options
Enable local daily backup:
Number of backups to retain:
10
Daily backup / cleanup time
Hour:
1 am
Minute:
0
Data Purging
Enable data purging:
Backup Configuration
Enable Kerberos keytab backup:
Enable Voice database backup:
SMB Backup
Enable SMB transfer:
Domainname:
Username:
Password:
Server name or IP address:
Server share name:
File to test SMB transfer:
Test Now
FTP Backup
Enable FTP transfer:
Destination host:
Destination subdirectory:
Username:
Password:
File to test FTP transfer:
Test Now
SFTP Backup
Enable SFTP transfer:
Destination host:
Destination subdirectory:
Username:
File to test SFTP transfer:
Test Now
Transfer to Secondary Appliance
Enable transfer:
Secondary appliance:
File to test SCP transfer:
Test Now
Automatic Backup
Download the public key and copy it to the remote server's /home/user/.ssh folder for the sftp transaction to function correctly. For the "Transfer to Secondary Appliance" option, download the public key, navigate to the second appliance, and upload the key using the upload key form.
Element Help
Please select the appliance type. The secondary appliance is typically used for storing backups from the primary appliance.

Configuring the Automatic Backup General Settings

Specify local machine backup options, an optimization schedule, data purging, or enable Kerberos keytab and Voice database backups in the general settings in Automatic Backups.

1. Select **Set Automatic Backup** in the **System Backups** page.
   The Setup an automatic backup page displays.



2. Configure the settings in the **Setup an automatic backup** dialog.

Field	Description
Appliance Type	Select the system that you wish to configure for backups. By default, Primary is selected. Select Secondary if you are logged into a system that will serve as a backup repository for Vocera files. This disables the backup functionality on the system, however, the number of backups to retain and the scheduled time for backup/cleanup can be configured.
Enable Daily Local Backup	Select this checkbox if you wish to store the database backup files on the local machine.
Number of backups to retain	Enter the number of backups to retain. The number of backups feature cannot be disabled; by default, the last 10 backups will be retained, however, you can retain as few as 1 or as many as 365 backup files.
Daily backup / Cleanup time	Select the hour (and minute, if desired) that the automatic backup will occur each day. Daily backups optimally should be performed during periods of low use, and in many facilities this may be between 01:00am and 03:00am. The daily backup time should be discussed with each facility to align with their resources, policies, and needs.
Enable data purging	Select this checkbox to delete the backed-up data from the local machine. This applies when an automatic backup is configured. When this option is selected, the **Enable local daily backup** box is checked and disabled automatically. This option is not available without enabling automatic backups, and once enabled, automatic backups cannot be disabled.
Enable Kerberos keytab backup	Select this checkbox to create backups of the Kerberos authentication's keytab files when performing system backups.

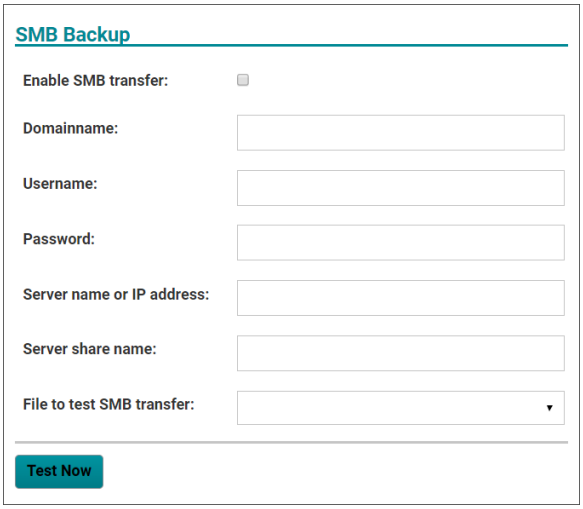
Field	Description
Enable Voice database backup	Select this checkbox to create backups of the Voice database when performing system backups.

3. Select one of the following to exit the **Setup an automatic backup** dialog:
   - Select **Apply** to save and implement the configuration choices.
   - Select **Cancel** to exit the page without changing the existing configuration.

Configuring an SMB Transfer of a Backup

Configure System Backups to automatically transfer the system backup files to another location for storage using Server Message Block (SMB).

1. Select **Set Automatic Backup** in the **System Backups** page.
   The Setup an automatic backup page displays.
2. Navigate to **SMB Backup** in the Setup an automatic backup page.



3. Configure the **SMB Backup** settings.

Field	Description
Enable SMB Transfer	Select this checkbox to use the SMB configuration.
Domainname	Enter the domain name for the location where the backup file will be saved.
Username	Enter the user name for the login credentials at the chosen backup location.
Password	Enter the password for the login credentials at the chosen backup location.
Server name or IP address	Enter the netbios name or server IP address for the chosen backup location.
Server share name	Enter the server path where the files will be stored in the chosen backup location.
File to test SMB transfer	Select the name of the backup file to test the SMB transfer capability from the dropdown menu in this field. The file name displays in the following format: extension_master_files –XXDATEXX-database.backup.

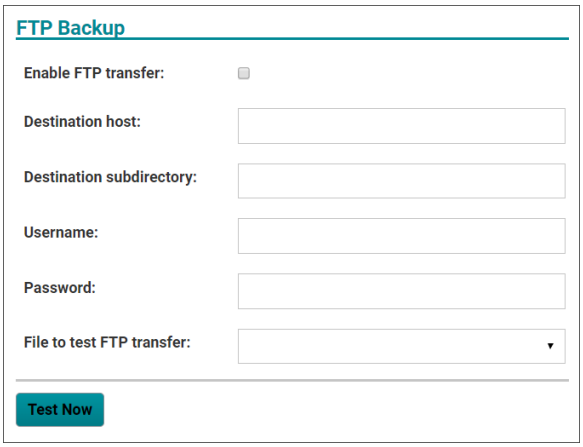
4. Select **Test Now** in the SMB Backup dialog to verify the configuration settings are correct in the system.
5. Select one of the following to exit the **Setup an automatic backup** dialog:

- Select **Apply** to save and implement the configuration choices.
- Select **Cancel** to exit the page without changing the existing configuration.

Configuring an FTP Transfer of a Backup

Configure System Backups to automatically transfer the system backup files to another location for storage using File Transfer Protocol (FTP).

1. Select **Set Automatic Backup** in the **System Backups** page.
   The Setup an automatic backup page displays.
2. Navigate to **FTP Backup** in the Setup an automatic backup page.



3. Configure the **FTP Backup** settings.

Field	Description
Enable FTP Transfer	Select this checkbox to use the FTP configuration.
Destination host	Enter the location where the backup file will be saved.
Destination Subdirectory	Enter the shared resource subdirectory location.
Username	Enter the user name for the login credentials at the chosen backup location.
Password	Enter the password for the login credentials at the chosen backup location.
File to test FTP transfer	Select the name of the backup file to test the FTP transfer capability from the dropdown menu. The file name displays in the following format: extension_master_files –XXDATEXX-database.backup.

4. Select **Test Now** in FTP Backup to verify the configuration settings.
5. Select one of the following to exit the **Setup an automatic backup** dialog:
   - Select **Apply** to save and implement the configuration choices.
   - Select **Cancel** to exit the page without changing the existing configuration.

Understanding SFTP Transfer of a Backup

Once automatic backups are configured, you may choose to transfer the backups to another location for storage using Secure File Transfer Protocol (SFTP).

SFTP public key authentication is a client authentication method often employed for automated file transfers, such as a Vocera system backup file transfer to a storage location.

In order for the SFTP transaction to authorize correctly, the public key on the Vocera Platform must first be stored in the authorized_keys file on the remote server where the backup is intended to be stored.

Note: Only Vocera Implementation Engineers and the facility IT Staff should have access to these directories; contact a System Administrator for assistance.

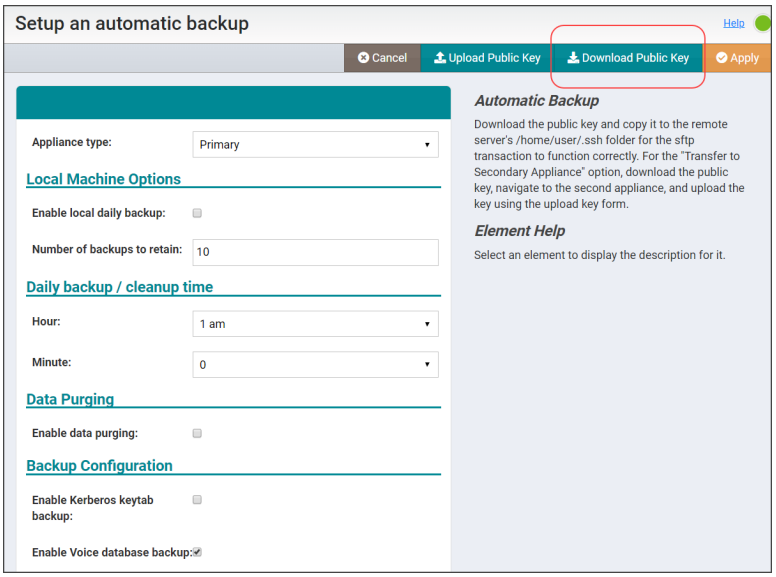
In the Vocera Platform Web Console, first download the public key found on the Vocera Platform, then save the public key in the authorized_keys file on the remote storage server.

Finally, configure the **SFTP Backup** settings in Automatic Backups to enable the transfer method for system backup files.

Using a Public Key for SFTP Transfer

Download the public key on the Vocera Platform, and then save the key to the authorized_keys file on the remote storage server.

1. Select **Set Automatic Backup** in the **System Backups** page.
   The Setup an automatic backup page displays.
2. Click **Download Public Key** in the Setup an automatic backup page.



   The **id_dsa.pub** key file appears in the system's Downloads folder.
3. On the server where you wish to store the backup files, use the command line program to navigate to the home directory for the user who will manage SFTP backups.
4. Locate the user's .ssh folder: **/home/username/.ssh**
   If needed, create an .ssh folder for the SFTP backups on the remote server as follows:
   a. Navigate to **/home/user**.
   b. Execute the following command line: **ssh-keygen –t dsa**
   c. Press the **Enter** key twice to create the .ssh folder.
5. Save the public key to the **authorized_keys** file on the remote storage server, as follows:
   a. On the remote storage server, execute the following command: **sudo nano .ssh/authorized_keys**
   b. Navigate to the Vocera system's Download folder, then open and copy the contents of the downloaded public key file: **id_dsa.pub**
   c. Paste the contents of **id_dsa.pub** into the **authorized_keys** file.
      Paste the contents on only one line, and do not allow breaks between spaces.

d. Save and close the **authorized_keys** file.

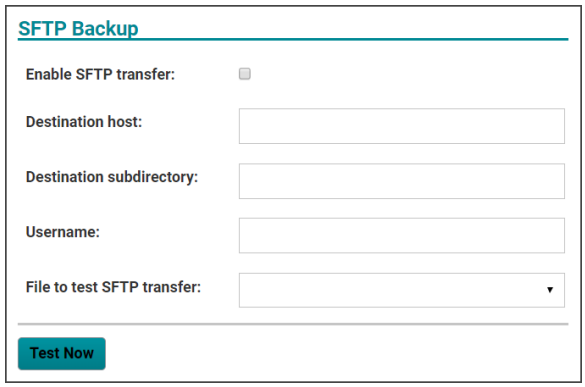
Next, configure the **SFTP Backup** settings in Automatic Backups to enable the system backup file transfer. Refer to Configuring an SFTP Transfer of a Backup on page 348 for details.

Configuring an SFTP Transfer of a Backup

Configure the SFTP transaction details in the automatic backup page of the Vocera Platform Web Console.

Locate the backup file from the Vocera Platform on the remote server under the specified user. The format of the file name should be similar to the following: **extension_master_files –XXDATEXX-database.backup**

1. Select **Set Automatic Backup** in the **System Backups** page.
   The Setup an automatic backup page displays.
2. Navigate to **SFTP Backup** in the Setup an automatic backup page.



3. Configure the **SFTP Backup** settings.

Field	Description
Enable SFTP Transfer	Select this checkbox to use the SFTP configuration.
Destination host	Enter the location where the backup file will be saved.
Destination Subdirectory	Enter the shared resource subdirectory location.
Username	Enter the user name for the login credentials at the chosen backup location.
File to test SFTP transfer	Select the name of the backup file to test the SFTP transfer capability from the dropdown menu. The file name displays in the following format: extension_master_files –XXDATEXX-database.backup.

4. Select **Test Now** in SFTP Backup to verify the configuration settings are correct in the system.
5. Select one of the following to exit the **Setup an automatic backup** dialog:
   - Select **Apply** to save and implement the configuration choices.
   - Select **Cancel** to exit the page without changing the existing configuration.

Understanding the Transfer of a Backup to a Secondary System

Once automatic backups are configured, you may choose to transfer the backups to another location for storage, such as a secondary Vocera Platform.

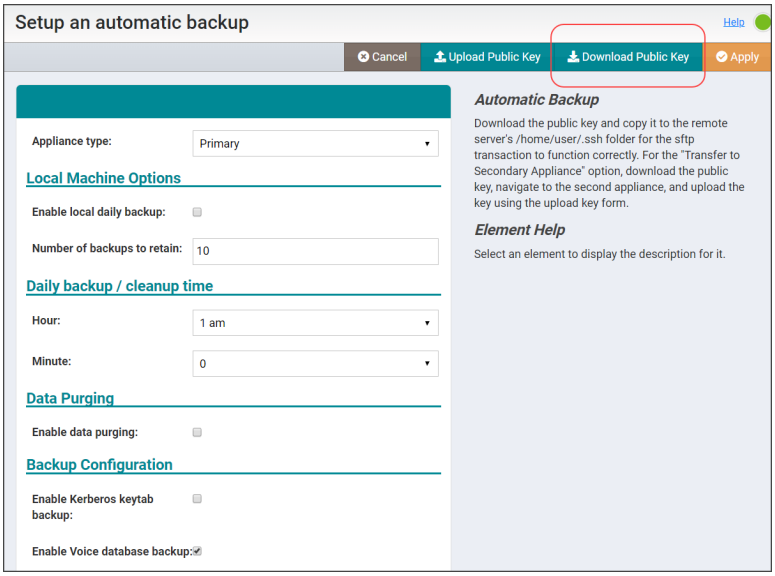
In order to transfer a system backup on the primary appliance to a secondary system for storage, first download the public key on the primary system. Then, upload the public key to the secondary appliance.

Finally, configure the **Transfer to Secondary Appliance** settings in Automatic Backups on the primary appliance to enable this method for transferring the system backup files to storage on the secondary appliance.

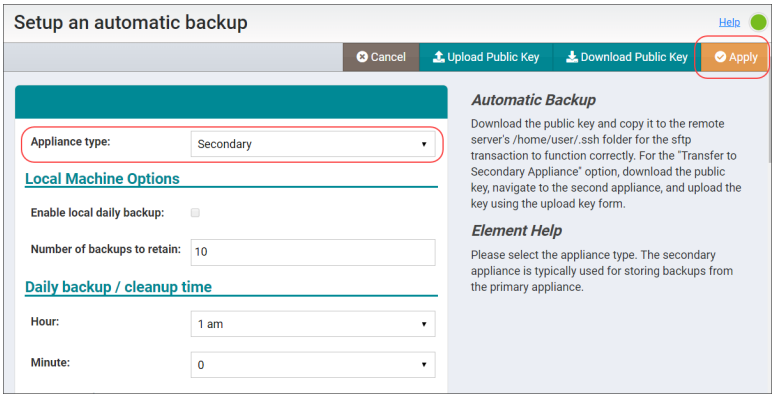
Using a Public Key for a Secondary Appliance Backup

Download the public key on the primary Vocera system, and then upload the public key to the secondary appliance used for storage of system backups.

1. In the primary system, select **Set Automatic Backup** in the **System Backups** page.
   The Setup an automatic backup page displays.
2. Click **Download Public Key** in the Setup an automatic backup page.

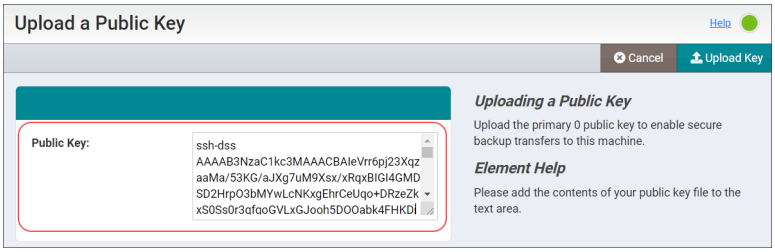


   The **id_dsa.pub** key file appears in the system's Downloads folder.
3. Navigate to the **id_dsa.pub** key file on the primary system in the Downloads folder, open it and copy the contents of the key file.
4. Log into the secondary system, navigate to **System Backups** and select **Set Automatic Backup**.
   The Setup an automatic backup page displays.
5. Select **Secondary** in the Appliance type field, and then select **Apply**.



   The Appliance type is changed from primary (default setting) to secondary on the storage system.
6. Select **Upload Public Key** in the **Setup an automatic backup** page on the storage system.
   The Upload a Public Key dialog appears.

7. Paste the contents of the primary system's **id_dsa.pub** public key saved above into the **Public Key** field.



8. Select **Upload Key** in the Upload a Public Key dialog. The available options are:
   - Select **Cancel** to return to the Setup an automatic backup page without making a change.
   - Select **Upload Key** to load the primary appliance's public key to the secondary appliance.

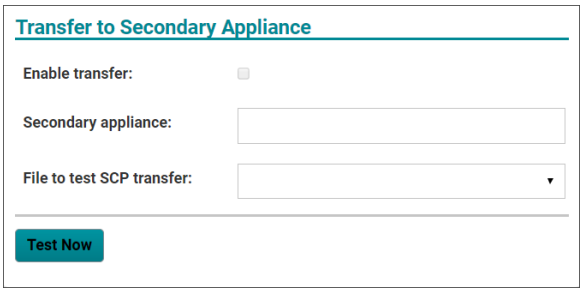
   The Upload a Public Key dialog clears.

Next, configure the **Transfer to Secondary Appliance** settings in Automatic Backups to enable the system backup file transfer. Refer to Configuring Transfer to Secondary System for a Backup on page 350 for details.

Configuring Transfer to Secondary System for a Backup

Configure System Backups to automatically transfer the system backup files to another location for storage, such as a secondary Vocera Platform.

1. Select **Set Automatic Backup** in the **System Backups** page.
   The Setup an automatic backup page displays.
2. Navigate to **Transfer to Secondary Appliance** in the Setup an automatic backup page.



3. Configure the **Transfer to Secondary Appliance** settings.

Configuration Field	Description
Enable Transfer	Select this checkbox to use the Transfer to Secondary Appliance backup information for the Vocera Platform.
Secondary appliance	Enter the IP Address or Fully Qualified Domain Name (FQDN) of the secondary Vocera Platform appliance.
File to test SCP transfer	Select the backup file to transfer to the secondary Vocera Platform appliance, using Secure Copy Protocol (SCP).

4. Select **Test Now** in the Transfer to Secondary Appliance section to verify the configuration settings are correct in the system.
5. Select one of the following to exit the **Setup an automatic backup** dialog:
   - Select **Apply** to save and implement the configuration choices.
   - Select **Cancel** to exit the page without changing the existing configuration.

High Availability

The Vocera Platform offers high availability (HA) feature to ensure that services are available for automatic fail over in a cluster.

Vocera Platform supports multiple High Availability nodes that share a virtual IP address to eliminate any single point of failure. The High Availability cluster configuration in the **Settings** section of the navigation bar allows you to configure your Vocera Platform appliance as a node within a cluster.

Understanding Clustering

Clustering is a mode of synchronous replication between two or more nodes to implement fault tolerance to your system.

Vocera Platform is focused on supplying a system for the delivery of contextual alerts and alarms without any downtime. The database (DB) and voice clustering features provide high availability to support your system in the event of a hardware or software failure.

In Vocera Platform a cluster maintains a virtual IP address (VIP) that acts like a cluster-manager. The VIP is always assigned to the active (master) node. All external traffic is targeted at the VIP and routed to the active node, automatically.

Before configuring a node for clustering, you must choose whether to create a new cluster or to join an existing cluster. If you are creating a new cluster, then that node becomes the master of that cluster. If you are joining a node to an existing cluster, then that node becomes a standby (slave) in that cluster.

The active node of a cluster sends out heartbeat/keepalive messages to announce its presence to the other nodes in the cluster. If a standby node fails to receive any heartbeat messages within a predefined time interval (default is 15 seconds), then it promotes itself to become the master of the cluster.

In the event of a failure, the system must be able to recover and continue to process information. Vocera Platform uses an active-passive high availability (HA) model to continue processing information. In an active-passive HA model, all data on the active node is replicated to all passive (Slave, or Standby/Backup) nodes. When failover occurs, the new active node takes over the Virtual IP (VIP) address assigned to the cluster, switches the database out of replication mode, and activates all adapters.

Cluster Management Tips

Review a list of best practices for cluster configuration and management.

You may want to follow these best practice recommendations before configuring the clusters:

- Add all necessary nodes at the time of cluster creation to avoid any unexpected failover.
- When setting up a cluster, it is critical to complete a single node's set up before you start configuring the next node.
- Configuring multiple nodes at the same time may cause the nodes to get out of synch with each other. After setting up a node, restart the node and verify the values are displayed correctly in the system.
- Limit the cluster size to two nodes, adding a third node to an existing cluster causes a failover between the existing two nodes in the cluster.

Configuring Clusters

Configure database and voice clusters from the Vocera Platform Web Console.

You can use **High Availability** in the **Settings** section of the navigation bar to perform the following tasks:

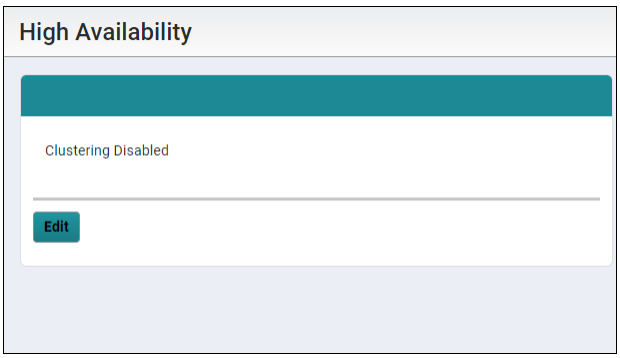
- Enabling clustering on a standalone node
- Joining an existing database cluster
- Changing the failover priority for servers in a cluster
- Removing a node from a cluster
- Accessing remote support in a cluster

For information on cluster status and failover configuration, see Database Cluster on page 122 and Voice Cluster on page 126.

Enabling Clustering on a Standalone Server

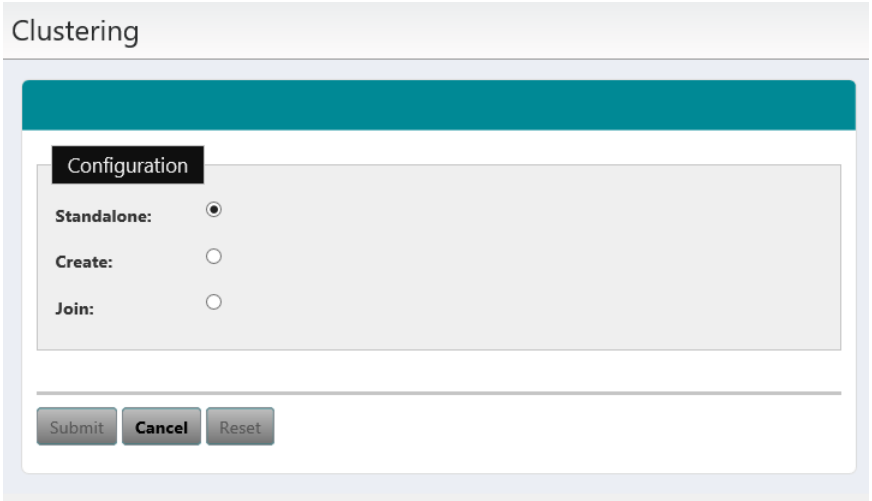
You can enable clustering on a standalone server from the Vocera Platform Web Console.

Vocera Platform is configured as a standalone node when clustering is disabled.

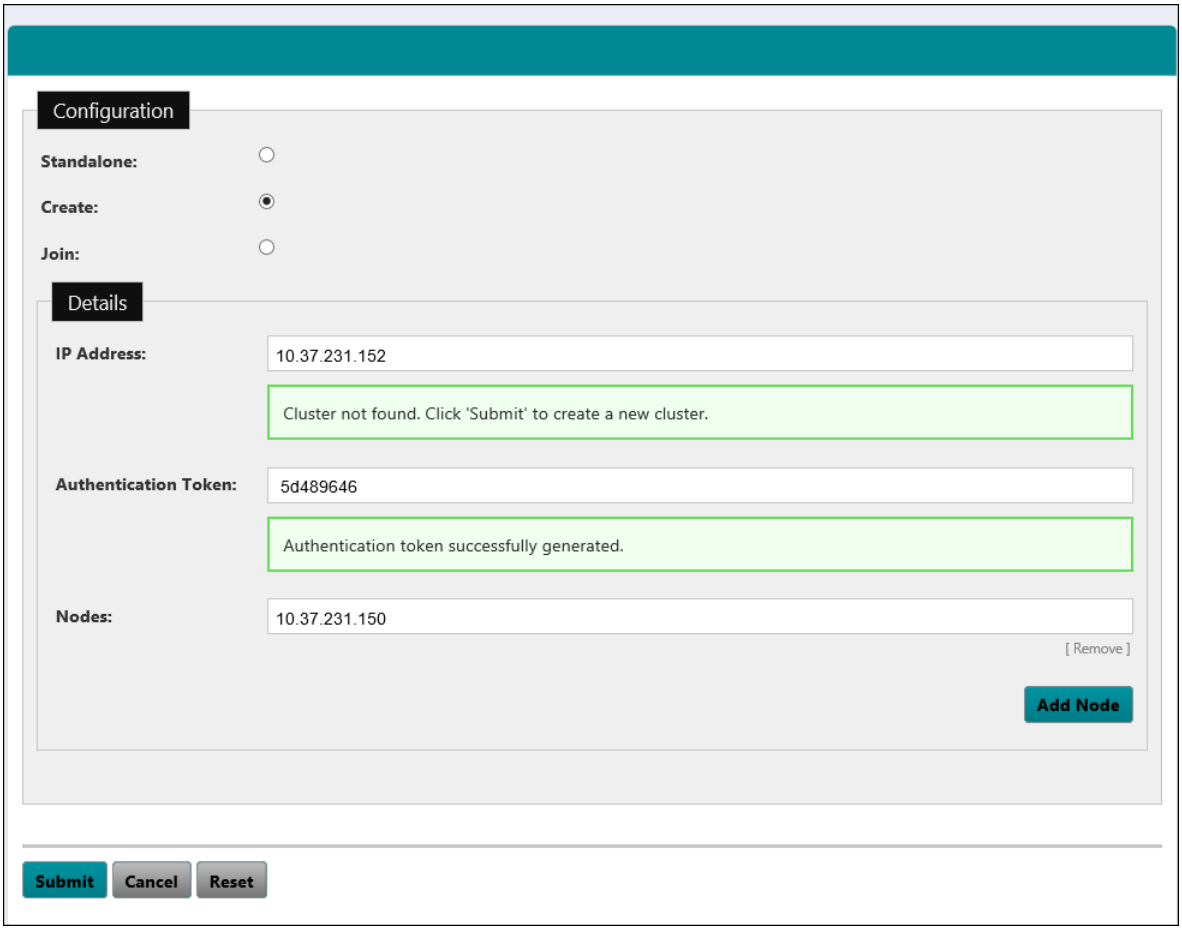


To initiate clustering in a standalone configuration:

1. Log in to the Web Console of your Vocera Platform master node.
2. Navigate to the **Settings** section in the navigation bar and click **High Availability**.
3. Click **Edit** to display the configuration information.
   The high availability configuration page displays.
   If your system is not a node in a cluster, you will notice that the clustering configuration is set to **Standalone**



4. Select the **Create** radio button to create a cluster.
5. Enter the Virtual IP (VIP) address in the IP Address field in the Details section.
   The system automatically generates the Authentication Token, once the IP Address field is populated.



6. Copy the authentication code.
7. Click **Add Node** and enter the IP address for the standby (slave) node.

   Remember: The recommended best practice is to add all known necessary nodes when you create the cluster.
8. Select one of the following to exit the configuration section:
   - **Submit** — to save changes and initiate cluster set up process.

- **Reset** — to undo any recent changes to the configuration fields.
- **Cancel** — to exit the cluster node configuration in a standalone state.

What to do next:

Enabling clustering is a two step process. After setting up the master node configuration, you must perform the configuration tasks on the slave node and allow it to join the cluster. For more information, see Joining a Database Cluster on page 354.

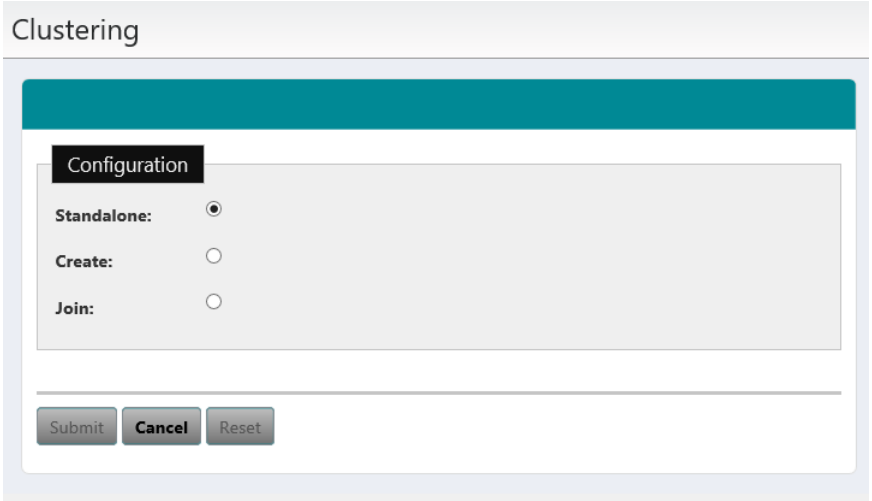
Joining a Database Cluster

After you add a node to the cluster, you must ensure that it joins the cluster.

Before a node joins the cluster, you must enable clustering. For information on enabling clustering, see Enabling Clustering on a Standalone Server on page 352

To join a node to the cluster:

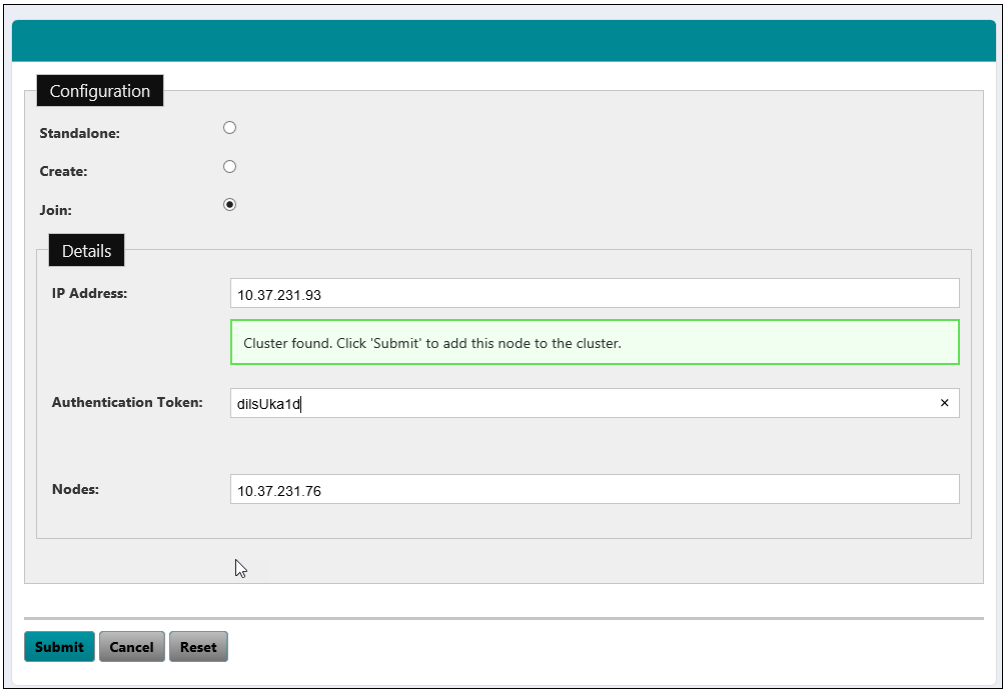
1. Open a new browser and log in to the Web Console for your slave node.
2. Navigate to the **Settings** section in the navigation bar and click **High Availability**.
3. Click **Edit**.
   You will notice that the clustering configuration is set to **Standalone**.



4. Click the **Join** radio button in the Configuration settings.
5. Enter or paste the authentication token in the token field. For more information on authentication code, see Enabling Clustering on a Standalone Server on page 352.
6. In the **Details** section, enter the following details:
   1. Enter the VIP or the Active (Master) node's PIP into the **IP Address** field.

      Note: The Slave nodes associated with the Master automatically populate in the **Nodes** field when the VIP or the PIP of the Master node is entered in the IP Address field.

   2. Enter the Master node's **Authentication Token** for the VIP or PIP.



7. Click **Submit** to save your changes to the system.
8. Launch the master node's Web Console on a separate browser.
9. Navigate to **Database Cluster** in **Status** section of the navigation bar.
10. Select the slave node and click **Repair Database**.

Changing the Failover Sequence

Learn the steps to change the failover sequence 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.

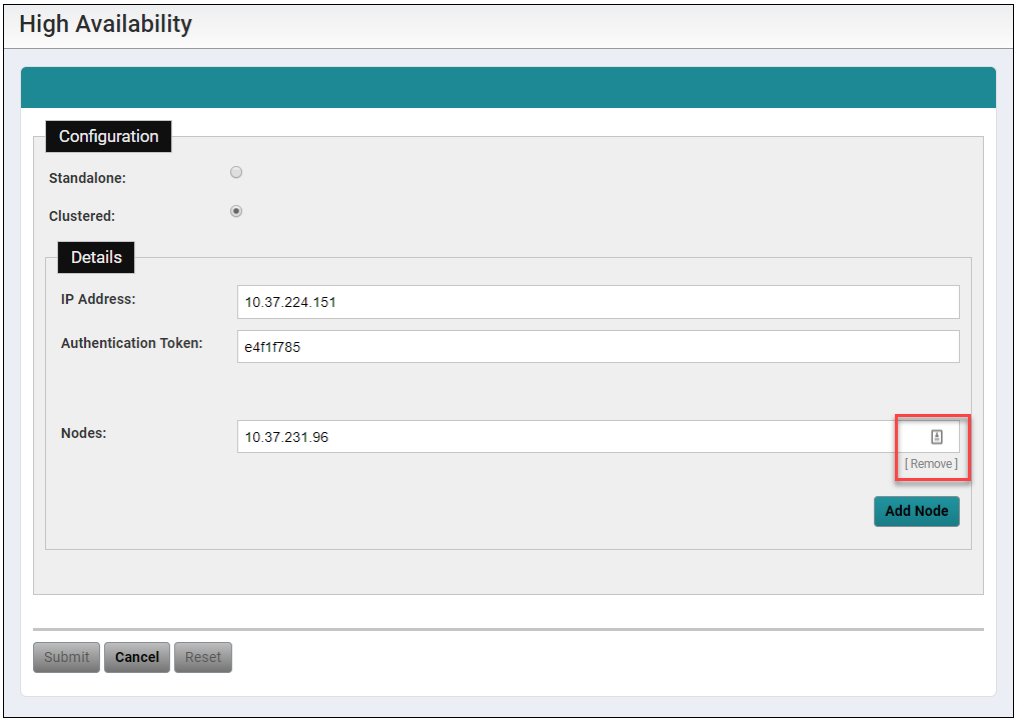
On some occasions, multiple standby servers may enter discovery mode at the same time. In this situation, the order in which servers are listed on the Cluster Setup page determines the order in which they will take control when failovers occur.

Removing a Node from a Cluster

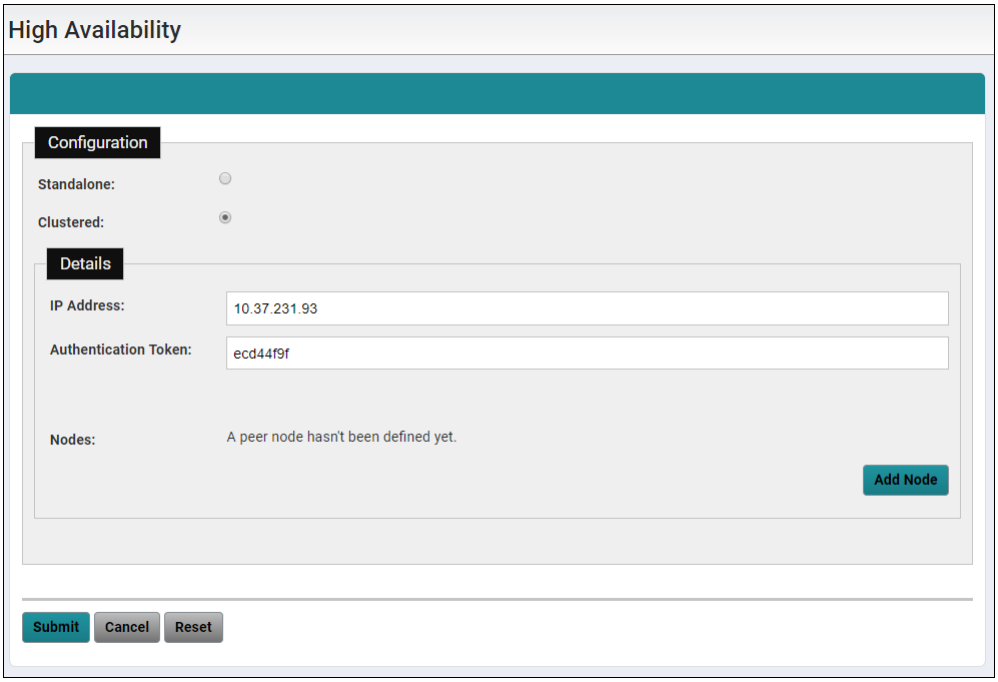
You can remove a node from the cluster and delete its association with the cluster settings.

To remove a node from a cluster:

1. Navigate to the **Settings** section in the navigation bar and click **High Availability**.
2. Click **Edit** to display the cluster setting details.
3. Click the Remove icon to remove the node from the cluster settings.



The High Availability dialog box refreshes and provides you the options to Submit, Cancel, or Reset the settings.



4. Select one of the following to exit the configuration section:
   - **Submit** — to save changes and remove the node from the cluster setting.
   - **Reset** — to undo any recent changes to the configuration fields.
   - **Cancel** — to exit the configuration without saving any changes.

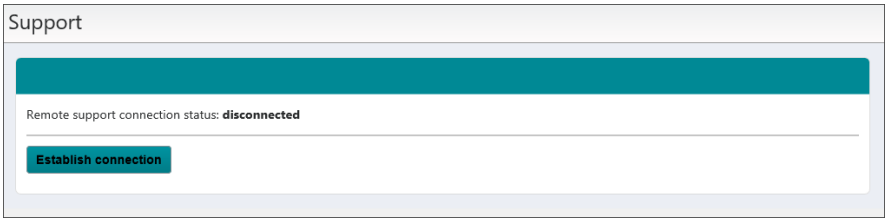
Accessing Remote Support in a Cluster

Remote support provides a secure way to grant a Vocera Support Specialist access to the Vocera Platform so that they can provide assistance.

In a clustered environment, you can set up support sessions with any node in the cluster. Once a support session is initiated, the Support page displays an alphanumeric connection ID; S#####, where # represents the digits in the ID.

When you contact Support, you must provide this ID to the support personnel in order to allow them access to your system.

1. Navigate to the **Security** section in the navigation bar and click **Remote Support**.
2. Click the **Establish connection** button and provide the connection ID to the support specialist.



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 Platform 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 **SMTP** settings in the **Destinations** tab to configure email address information for alerts. For more information, see Configuring SMTP Settings on page 110.

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.

Cluster Health Checks

Manual checks on the overall health of a high availability cluster should be performed to prevent service disruption at a customer site.

In the Cluster tab, the Status panel provides a view of the overall health of the cluster. Additional preventative manual health checks must be performed before a system can be implemented successfully, and to ensure that known issues do not occur at a customer site.

The Status panel displays the state of each node in the cluster, but it is unable to report everything about the overall health of the cluster. This appendix information provides preventative actions that Implementation Engineers should perform to prevent service disruption at a customer site. Perform these health checks as early as possible to catch any problems, before the system is allowed to go live at the customer site.

This health check information is specific to high availability clustering and is not intended to be general purpose troubleshooting information. Use the information in this section to obtain a more accurate status on the cluster.

F5 BIG-IP Health Check Configuration for a Cluster

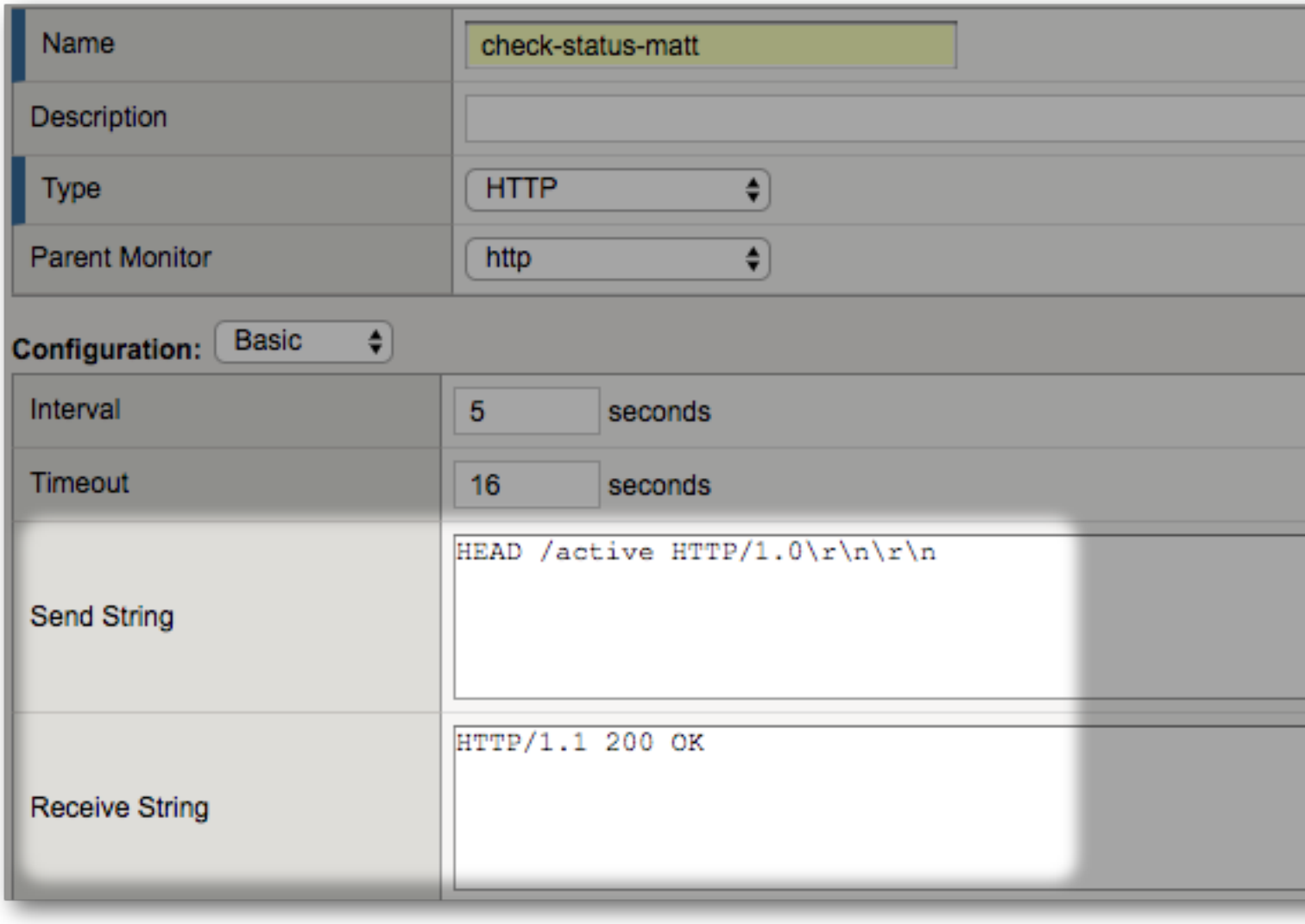
An F5 BIG-IP system can be configured to monitor a Vocera Platform cluster.

The F5 BIG-IP system is not supported or managed by Vocera; configuration of a third party vendor such as F5 is the responsibility of the customer. The customer must ensure that their System Administrator is fully qualified to administer the F5 BIG-IP system.

This F5 BIG-IP configuration information is provided for the customer's technical team to gain an understanding of some concepts needed prior to an installation. Access the F5 company website for assistance.

The F5 BIG-IP system monitors the Vocera cluster in order to seamlessly track the Master node in a failover. A health check indicator reports which of the nodes is the current Master. For this communication to happen, ensure that the following configuration is correct on the BIG-IP system.

Configure the ADC system to send a "HEAD / active" query to the default webpage on a cluster node, and receive a response from the active server of "200" or "200 OK" as shown in the example below. The inactive nodes will not respond with the configured response code and will be marked as Offline, allowing traffic to be directed only to the node that responds with the configured code.



Example Configuration for Vocera Platform and an ADC

Example configurations for Citrix Netscaler, F5 BIG-IP, and CUCM and SpectraLink XML deployments are available.

The configuration instructions are generic and universal to the Vocera Platform product, and are provided as an example only.

Contact Vocera Support Services for assistance if needed.

F5 BIG-IP Deployment with CUCM and Spectralink XML

Vocera Platform connects through the F5 ADC to interface with these external systems.

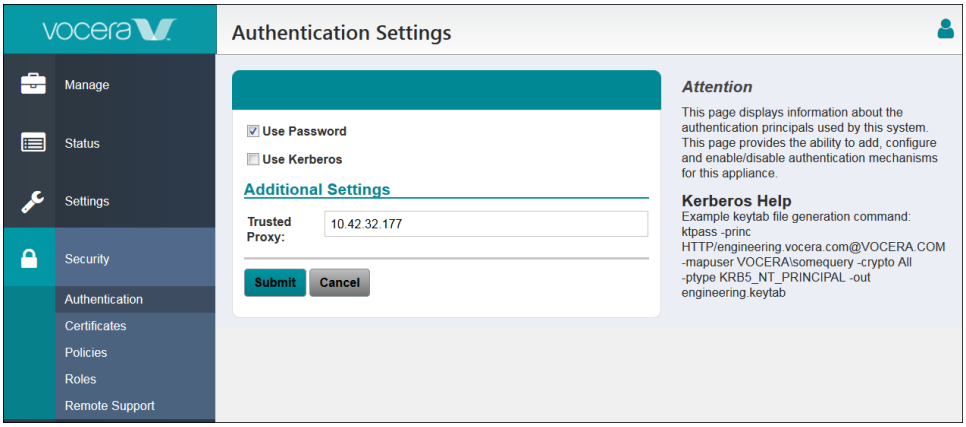
In the Third-Party ADC Deployment Model diagram, there are network elements which will connect to the ADC instead of directly connecting with Vocera Platform; instead the system connects through the ADC to interface with the external systems. For example, external systems such as ResponderSync, TAP, and HL7 will all need to communicate with Vocera Platform, but they will connect directly to the ADC. From a network perspective, when the Vocera Platform connects to the external system (i.e., ResponderSync), the system sees the IP address of the ADC, not the IP address of the external system.

In most cases, the external system communication can be relayed through the ADC where the ADC controlls the IP address without any problems. For some systems, however, the external system's IP address is required for Vocera Platform functionality. With both CUCM and SpectraLink XML external systems, for example, the Vocera Platform needs the external IP address to correlate the registration status of a device with the external system. Normally, the Vocera Platform cannot access the external IP address, as the ADC address is proxied instead. In these cases, there is a special requirement that the Vocera Platform will need knowledge of the remote IP address for those devices that the Vocera Platform connects to.

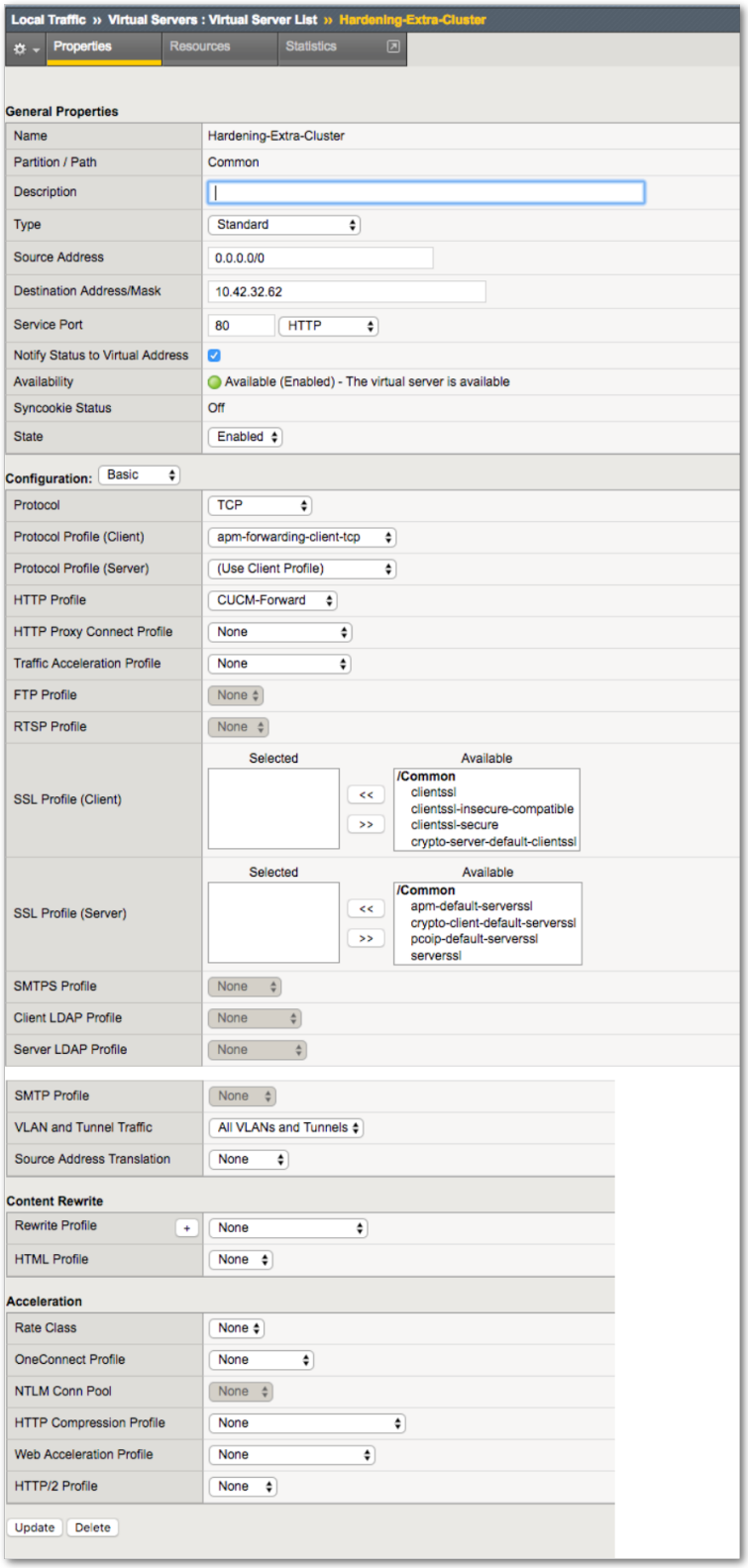
The requirement is to configure BIG-IP to carry in its data payload the information for the remote address for the device. This configuration means that even though the direct connection is with the ADC and not the device, inside the data payload, encoded in the data, is the remote address **ADDR** of the device. Using the configuration shown below, the Vocera Platform can find the IP address, extract it, and marry it to the CUCM exchange. That way, when the system needs to communicate with the device directly, to change the registration status or send something to the device, then using the exact IP address that was encoded in the data payload, the correct device can be accessed.

The following configuration is required on the F5 BIG-IP server for both CUCM and SpectraLink XML adapters. The HTTP proxy (VIP on BIG-IP) is required to include X-Forwarded-For in the header.

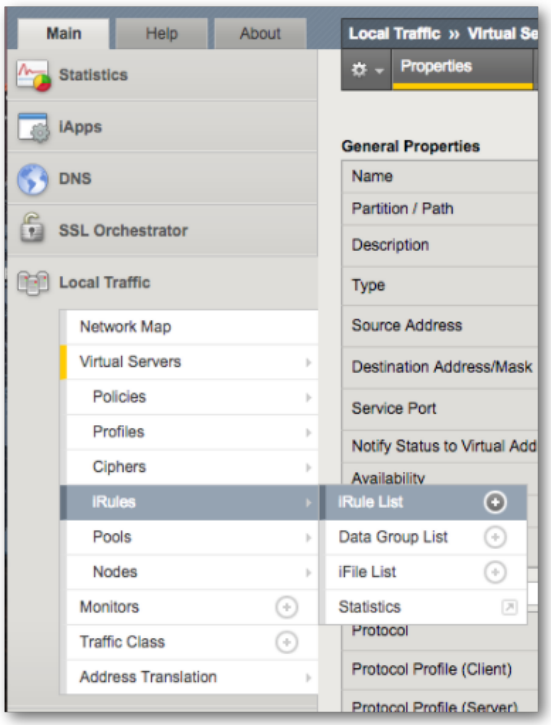
On the Vocera Platform, navigate to Authentication Settings (**Security** > **Authentication**). In the "Trusted Proxy" field, enter the SNAT address of the VIP.



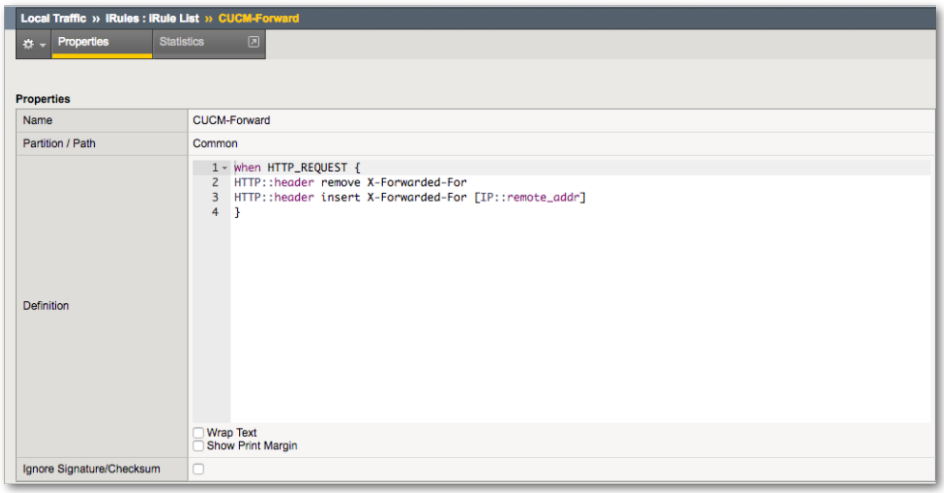
In BIG-IP, first create the virtual server. Specify the Name, Type, Source Address, Destination Address, Service Port, Protocol, Protocol Profile and HTTP profile fields, and then click the **Update** button.



Next, configure an iRule in BIG-IP: Navigate to **Local Traffic** > **iRules** > **iRules List**, and then click **Create**.



Finally, the header insert, shown in line 3 in the Properties window, is used to configure BIG-IP to carry in its data payload the information for the remote address for the device. The HTTP proxy (VIP on BIG IP) is required to include X-Forwarded-For in the header.



HA Deployment Configuration Selection

Vocera Platform provides a high availability (HA) feature for automatic fail over in a cluster.

When the primary server or node in a cluster experiences a failure, the system will fail over from a primary server to a standby server. HA clusters use a heartbeat signal sent over the network for health and status monitoring of the cluster. Vocera Platform provides an active-passive model with the following two options to manage the VIP:

- Vocera Platform manages the network requirements for the VIP
- A third system, such as a load balancer (ADC), manages the VIP with a different set of network requirements

Unlike other complex systems that follow an active-active HA model to distribute the load between multiple servers, the Vocera Platform follows an active-passive model. Which means, the entire workload is directed to one single server (with a valid IP address) and cannot be shared across multiple servers.

The following two network arrangement types can be configured:

A) Layer 2 Adjacent Deployment Model on page 363: All nodes in the cluster are all located within the same IP subnet; i.e., the primary and all standby servers are Ethernet Layer 2 Adjacent to each other.

B) Third-Party ADC Deployment: One or more nodes in the cluster are not in the same subnet as the others; i.e., at least one node is required to traverse through a network router in order to connect to the other nodes in the cluster.

Layer 2 Adjacent Deployment Model

The Layer 2 adjacent deployment provides the most direct and simplest method for the cluster to manage the VIP.

The primary server on the cluster responds to connections addressed to the VIP. All external connection requests are directed and serviced by the primary server. In this configuration, there is no need for a third-party server (i.e., load balancers, application delivery controllers, etc.) to manage the VIP; the cluster itself manages the VIP.

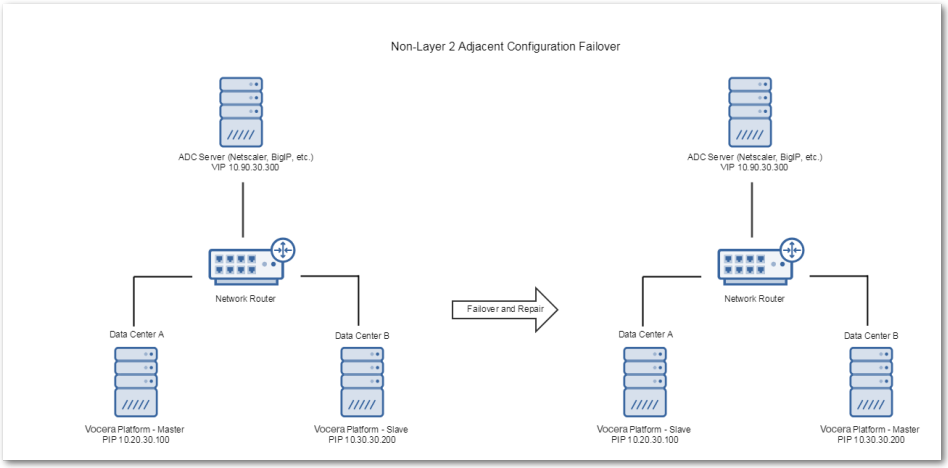
As shown in the following diagram, if the primary server fails or becomes disconnected, then the secondary server assumes the role of the primary and begin to respond to connections on the VIP address. In this example, the nodes in the cluster share a VIP as they change standby and primary roles.

Third-Party Load Balancer (Non-Layer 2 Adjacent) Deployment Model

In a third-party load balancer deployment, the cluster does not directly respond to or manage the VIP.

In a Non-Layer 2 Adjacent deployment, the cluster does not directly respond to or manage the VIP. In this configuration, a third-party load balancer such as the application delivery controller (ADC) is necessary. The ADC will respond to the VIP address and direct those connections to the primary server in the cluster. The cluster provides an indicator that allows the ADC to determine which particular node in the cluster is the primary.

During a failover event, as shown in the diagram below, the standby node with the highest priority assumes the primary role. The indicator for that node will reflect the new status, allowing the ADC to begin to direct connections to it. In this example, the VIP remains with the ADC while the cluster nodes change standby and primary roles.



FAQs for HA Decisions

Logical questions to ask regarding the most appropriate choice for managing the public VIP in your Vocera Platform system.

Why do I need a VIP in my facility?

The Virtual IP (VIP) is the address that represents the public network identity of the cluster.

The Virtual IP (VIP) is the address that represents the overall cluster and is intended to be used for all third-party system and device integrations. The VIP is the only address that should be shared with other systems that require integration with Vocera Platform, since it represents the public network identity of the cluster.

For an Ethernet Layer 2 Adjacent deployment, the VIP is normally assigned to the master node within a cluster. During a failover event, the VIP is assigned to another node that is taking over the master role at that time. The VIP is not intended to be permanently and irrevocably assigned to an individual server while in a cluster, but rather it is managed by the cluster; it "floats" from one node to another during failover events. In addition to the VIP, each node in the cluster also has its own unique IP address, different from the VIP, that is assigned permanently to that node. While a node is a member of a cluster, it will use the private IP address to communicate with the other nodes in the cluster in order to maintain the overall cluster function and arbitrate role assignment during failover events. Reassignment of the VIP from one server to another during a failover is an automatic action carried out by the cluster itself and does not require user intervention.

For a Non-Layer 2 Adjacent type deployment, the VIP is assigned to the ADC. The ADC itself can be deployed as either an individual server, or as its own cluster of nodes to provide robustness for the ADC services. In this scenario, the VIP is managed externally by the ADC with the local customer's HA policy, and the Vocera Platform nodes will only have their private IP assignment, regardless of their current role. In addition to managing the VIP, the ADC will redirect network connections from third-party integration systems from itself to the master role in the Vocera Platform cluster for processing. The ADC is able to determine the master role assignment by monitoring all nodes in the cluster, as the node with the master role assignment will return a positive indication. During a failover event, the master node stops sending a positive indicator, then another node will take on the master role, and then transition its monitor return value to positive. At that time, the ADC will transition its network connections from the failed master to the new master node, completing the failover event.

What are the network requirements for the non-ADC deployment model?

Layer 2 Adjacent deployment requires that nodes share a subnet.

The Vocera Platform and the supplied VIP must reside on the same subnet; i.e., given the VIP address may be assigned to any node in a cluster, all nodes all have to share one common subnet. See the Ethernet Layer 2 Adjacent deployment description.

Why can't the non-ADC model be deployed across two different data centers with different subnets?

When the servers are in different subnets, then they cannot time share an IP address between them.

In order for the IP address to "float" between one server and to another, it has to be a valid IP that can exist in either server. The servers need to be in the same subnet to share an IP address between them.

How can I support a multiple data center deployment without Ethernet Layer 2 Adjacency between them?

Solution may be to implement a third party ADC, or upgrade the shared network.

One possible solution is to introduce a third party ADC to solve the problem of redundancy between the two data centers. See the Non-Layer 2 Adjacent type deployment section in this page.

Alternatively, the network between the two datacenters could be upgraded to support Ethernet Layer 2 Adjacency by one of several method options as described in How do I span Layer 2 Adjacency across the data centers?.

How do I span Layer 2 Adjacency across the data centers?

Your organization will need to evaluate its own infrastructure to determine an appropriate method of spanning Layer 2 Adjacency across the data centers.

There are a variety of technologies and products that support creating Layer 2 Adjacent networks across geographically separated dataceters. Some examples are Multiprotocol Label Switching (MPLS) supported by enterprise grade network equipment, or network virtualization overlay products such as VMware NSX. These approaches will require an investment of time, money, and effort to implement. Research and evaluate the available options to determine the best solution for your organization.

Can a third element manage the public VIP when nodes are on two different subnets?

An ADC solves the problem of nodes in two different data centers with no common subnets.

The ADC is a third element that manages the public VIP, which is the front network point to the two (or more) individual nodes in the cluster.

See the two diagrams in HA Deployment Configuration Selection for a view of a Layer 2 Adjacent failover, and failover with a third-party ADC. Using Layer 2 Adjacency is simpler; it has fewer elements, making it more reliable, robust, easier to maintain, and it also provides a faster failover convergence time.

An ADC is a more complex solution with more elements to implement, configure, troubleshoot, and maintain. In addition, this complex system requires more failover convergence time. Furthermore, there is a significant investment of time, money, and effort to implement a complex ADC solution, as this is a major endeavor.

Failover convergence time is counted from the moment that something goes wrong with the master server, to the time that the new master server is in a steady state and able to receive and service all the connections that were broken from the failure. This convergence time is always longer with an ADC, all factors being the same, than the simpler Layer 2 Adjacency system failover.

Can the Vocera Platform support my ADC?

Vocera Platform supports F5 BIG-IP and Citrix NetScaler.

Vocera Platform has been tested and validated against these solutions. Other ADCs may perform in a similar way to these products, but Vocera cannot provide technical guidance or support for products that Vocera Platform is not validated against.

If your company uses another ADC, reach out to your Vocera representative who will follow up with the Vocera Product Management team to investigate the technical feasibility of supporting other ADCs.

When our facility is not using an ADC, can I determine when an adapter and/or the system is performing as expected?

Yes, Vocera Platform offers a robust SMTP, SNMP, and syslog alerting system to notify the facility of an issue on a system component.

SMTP, SNMP, and syslog alerting for system components is available through the Audit Log in the Vocera Platform Web Console. Please see Accessing Database Audit Event Logs for additional information.

When our facility is using an ADC (load balancer), can I determine when the master is available and responding as expected?

You can view the status of the master node in Vocera Platform.

Using the VIP, log into Vocera Platform to review the cluster status panel displays with the details for each node. If the VIP is unresponsive then the issue may be either on the cluster itself or in the ADC configuration, and would require further investigation.

What is the failover time?

Failover time (also known as "convergence time") is the elapsed time between the master role transitioning from one cluster node to another.

Comparing the two possible deployment configurations, the Ethernet Layer 2 Adjacent deployment setup offers the shortest failover time because it does not incur the additional overhead of the ADC. For additional information about the ADC setup, see Non-Layer 2 Adjacent type deployment.

Will any of my data be lost during a failover?

In edge cases, some data that is being processed may be lost during a failover.

In the event of a failover, in flight messages may be lost in certain scenarios. These edge cases can be mitigated by configuring escalations within Vocera Platform and by having the sending system resend messages in the event of a failure.

Badge Properties Editor

Badge Properties Editor is a tool that allows you to set properties for the badge and lets it connect to the wireless network.

Using the Badge Properties Editor

Badge Properties Editor (BPE) is a tool that allows you to set properties for the badge and lets it connect to the wireless network.

The Badge Properties Editor (BPE) is installed on both the configuration computer and the Vocera Voice Server computer. If you are performing initial badge configuration, use the Badge Properties Editor on the configuration computer.

To use the BPE, perform the following tasks:

1. Locate and double-click the **Vocera BPE Launcher** icon on the desktop the first time. For subsequent logins, access the **Vocera BPE Launcher** using the URL **http://127.0.0.1:8011/#!/** where `127.0.0.1` is the localhost and `8011` is the Voice Server IP port for BPE.
   The Badge Properties Editor UI appears.
2. Select a badge you want to configure, under Badges.
   The badges you can configure are:
   - B2000
   - B3000
   - B3000n
   - V5000

   Note: The B2000 badge is not supported on Vocera Platform 6.1.0
3. Set the following badge property values for your badge:
   - **Profiles**—This parameter is applicable only for B3000n badge. Specifies the name of the file to control general behavior. You must use the `profiles.txt` files for environments that require more than one wireless profile in a dynamic campus-type setting.
   - **General Settings**—Specifies the minimal set of properties you need to set for any badge in use at your site. You must set values for all the general properties. Depending on the configuration of your site, you may have to set other properties.
   - **Security Settings**—Specifies how to enable badges to work with the security features that correspond to the type of authentication and encryption employed by your wireless network. If you are deploying different types of Vocera badges, you can configure them to reside on separate SSIDs and take advantage of the enhanced security support offered by newer badge models. If all the badges reside on the same SSID, the security you opt must be supported by all badge types.

- **Wireless Settings**—Specifies the parameters that affect how the badge operates on the wireless network of your organization. A set of WLAN parameters can be scanned through for connectivity in different locations. Wireless clients learn about available APs by scanning other 802.11 channels on the same WLAN or SSID.
- **Custom Properties**—Specifies the customized badge properties you want to upload to the badge. The options available are:
  - **Select**—Select the badge property that you want to configure.
  - **Key**—Enter the key in the following format-`B2.<Property-Name>`, `B3.<Property-Name>`, `B3N.<Property-Name>`, and `V5.<Property-Name>` for B2000, B3000, B3000n, and V5000 respectively.
  - **Value**—Enter the value of the property.
  - **Comment**—Add comments for your reference.

Note: Key and Value fields are mandatory.

4. Click one of the following:
   - **Submit**—Allows you to submit the changes.
   - **Discard Changes**—Allows you to discard the changes and re-enter the badge properties.

   The Badge Properties Editor creates a `badge.properties` text file under `\vocera\config`.

   You can now upload the badge properties to your badges.

B3000 Badge Properties Configuration

This section lists the badge properties that you can configure using the BPE on your B3000 Badge.

Enter information or check the following badge properties:

Fields	Description
Profiles	
Selected Profiles	Specifies the name of the profile you selected to control general behavior. You must use the `profiles.txt` files for environments that require more than one wireless profile in a dynamic campus-type setting.
Create Profile	Allows you to create a new profile to control general behavior.
General Settings	
Server IP Address*	Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field. Use dotted-decimal notation to specify this value. For example, `192.168.3.7`. If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces. **Note:** Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.
SSID*	Specify an SSID other than vocera (all lower-case) for your production server. Badges are factory-programmed to use the vocera SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.

Fields	Description
Hide Boot Menus	Specifies the option to prevent configuration menus to be displayed on a badge. The menus provide access to powerful utilities for maintenance and troubleshooting. Use these utilities only when you are working with Vocera Technical Support. **Note:** This property is ignored by the B3000 and B3000n badges, with menus always hidden.
Group Mode	Specifies the option to ensure noise-canceling microphones are turned off while users are on a call. Group Mode widens the speech zone, allowing additional people to speak into the primary microphone of the badge. Uncheck this option if you want to eliminate background noise when users are on a call. **Note:** B3000 and B3000n users can change the Group Mode setting on their badges, overriding the default. • For B3000: Group Mode is always off during Genie interactions and broadcasts. • For B3000n: Group Mode is automatically enabled when the badge is turned to a 105-degree angle to improve voice recognition.
Reset Volume to Default	Specifies the option to reset the default volume at boot-up. Otherwise, the previous volume setting is maintained at boot-up.
Security Settings	
Enable FIPS	Specifies the option to enable the badge cryptographic security module to run in a secure mode that conforms with Federal Information Processing Standard (FIPS) 140-2. When **Enable FIPS** field is checked, it requires WPA2-PSK, WPA2-PEAP, or WPA2-TLS.
Authentication Type	
Open	Specifies that your wireless network does not require authentication.
LEAP	Specifies that your wireless network implements the Cisco LEAP protocol for authentication.

Fields	Description
Username and Password*	Enter appropriate values in the **Username** and **Password** fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication. If your network uses EAP-TLS authentication with external certificates (instead of the Vocera Manufacturer Certificates), enter a value for the **Username** field but not the **Password** field. Otherwise, skip both these fields. Each badge on a Vocera Voice Server must use the same username and password. The username format depends on the requirements set by the RADIUS authentication server. For example, when you use LEAP with Cisco ACS and Windows Active Directory, enter domain \ userid in the **Username** field, where domain is a Windows domain name and userid identifies the user. Other RADIUS servers may require the username only. The password value is case sensitive. You can use initial or embedded spaces in either of these values; trailing spaces cause an error message when the values are saved. The badge supports a maximum of 128 alphanumeric characters for the **Username** and 32 alphanumeric characters for the **Password**. In addition, the badge supports the following characters for LEAP passwords: `^ # ! * @ % & $` **Note:** If you are using EAP-FAST authentication and you change the username or password values, you must also generate a new PAC file. With manual PAC provisioning, you must generate a new PAC file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer. With automatic PAC provisioning, you must restore the factory settings on the badge and reconfigure it. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.
WPA-PSK	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication.
Pre shared Key	If Authentication Type is set to **WPA-PSK**, the pre-shared field appears. The pre-shared key that the badge supplies for authentication is a 64-character, hexadecimal value.
WPA-PEAP	Specifies that your wireless network uses the WiFi Protected Access Protected Extensible Authentication Protocol for authentication.
EAP-FAST	Specifies that your wireless network uses Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling for authentication. EAP-FAST authentication enables you to select between automatic or manual PAC provisioning.
Enable Auto-PAC	Specifies the option to enable automatic download of a PAC from the Cisco ACS, and the ACS periodically refreshes the PAC to ensure it does not expire. To take advantage of automatic PAC provisioning, you must configure badges correctly by setting Auto-PAC properties. If you enable manual PAC provisioning, you must create a `.pac` file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer.
Provision Auto-PAC on Expire	Specifies the option to enable automatic provisioning of a new PAC when it expires. If this property is unchecked, a badge with an expired PAC displays the following message: "Expired or invalid PAC credentials." **Note:** This message appears only if a badge has been powered off or did not roam at all for a while and the master key and the retired master key on the Cisco ACS have expired. If this happens, the badge must to be reconfigured. To take advantage of this feature, you must also select EAP-FAST authentication.

Fields	Description
Auto-PAC Provision Retry Count	Specifies the option to limit the number of times a badge attempts to retry retrieving a PAC from the Cisco ACS after the first attempt failed. For example, the badge attempts to retry retrieving a PAC due to wireless network problems. Select a number from 0 to 5. If a badge exceeds the retry count, it displays the following message: `Too many retries for Auto-PAC provisioning`. By default, this property is set to 0 (indicates no retries). To take advantage of this feature, you must also select EAP-FAST authentication.
EAP-TLS	Specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication. Check the **EAP-TLS** field to enable the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your self-signed certificates or obtain them from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS. Alternatively, uncheck this box to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Computer. Vocera Manufacturer Certificates use 2048-bit RSA keys that provide excellent security for enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server. For more information on security certificates, refer to Vocera Device Configuration Guide.
Use Custom EAP-TLS Certificates	Specifies the option to enable the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your self-signed certificates or obtain it from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS, and specify the **Username** and **Client Key Password** properties. Alternatively, uncheck this box to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Computer. Vocera Manufacturer Certificates use 2048-bit RSA keys that provide excellent security for enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server. This property is available only when the **Authentication** property is set to EAP-TLS.
Encryption Type	The encryption types available are: • TKIP-WPA—Specifies your network uses TKIP as defined by WPA. • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2 Use hexadecimal characters to enter the key that the access point is using.
Wireless Settings	
2.4 GHz Channels	
Set to Defaults (1, 6, 11)	Specifies the option to force badges to scan the three non-overlapping 2.4 GHz channels of 1, 6, and 11.

Fields	Description
Specify Channels	Specifies the option to specify up to four arbitrary channels to scan. If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select **Specify Channels** and enter the specific channel numbers in a comma-separated list. Ensure that you specify only channels that are supported for your locale.
Roaming Policy	The **Roaming Policy** property specifies how quickly a badge searches for an access point when signal quality drops. Higher values cause a badge to search sooner and may correct problems with choppy audio. However, a badge cannot send or receive audio packets while searching for an access point, as communication may be interrupted. Lower values allow a badge to tolerate lower signal quality before searching. The optimal threshold value varies from one 802.11 network to another, depending on how the network is configured. Select a value from 1 to 5. The default value is 2.
CCKM	Check **CCKM** box if you want to enable Cisco Certified Key Management. CCKM is a form of fast roaming supported on Cisco access points and various routers. Using CCKM, Vocera devices can roam from one access point to another without any noticeable delay during reassociation. After the RADIUS authentication server initially authenticates a Vocera device, each access point on your network acts as a wireless domain service (WDS) and caches security credentials for CCKM-enabled client devices. When a Vocera device roams to a new access point, the WDS cache reduces the time it needs to reassociate. To take advantage of this feature, your access points must also support CCKM, and you must use either LEAP, WPA-PEAP, EAP-FAST, or EAP-TLS authentication.
802.11d	Check **802.11d** box if you are in a country where systems that use other standards in the 802.11 family are not allowed to operate.
Custom Settings	
B3.BroadcastUsesIGMP	Vocera broadcast is implemented as IP Multicast. If broadcast commands must cross a subnet, IGMP must be supported in the switch or router. Set this property to TRUE.
B3.ClosedMenus	Specifies whether the badge configuration menus are hidden, or if they can be easily accessed through the DND button: • **FALSE** specifies that you can access the configuration menus by pressing the DND button within three seconds displaying the boot countdown timer. • **TRUE** specifies that you must use the special sequence of button presses to display the configuration menus. This value prevents displaying configuration menus and inadvertently causes configuration problems in a badge.
DefaultHandsetVolume	Lists the default volume level of Privacy Mode when no users are logged in.
DisplayHandsetMode	Displays Privacy Mode on the badge menu under Settings.
B2.EnableAPSD	Specifies whether the badge takes advantage of the Unscheduled Automatic Power Save Delivery Subset (U-APSD) of 802.11e. U-APSD improves power management and potentially increases the talk time of 802.11 clients. • **FALSE** specifies that U-APSD is disabled. • **TRUE** specifies that U-APSD is enabled. To take advantage of this standard, your access points must support it. **Important:** Both the **B3.EnableAPSD** and **B3.EnableWMM** properties must be set to the same value.

Fields	Description
B3.EnableWMM	Specifies whether the badge takes advantage of the WiFi Multimedia (WMM) subset of 802.11e. The 802.11e QoS provides standards-based QoS to prioritize voice over data traffic and ensure high-level voice quality. • **FALSE** specifies that 802.11e QoS is disabled. • **TRUE** specifies that 802.11e QoS is enabled. To take advantage of this standard, your access points must support it, switches and routers must be configured to honor DSCP markings, and the Vocera QoS Manager service must be enabled on the Vocera Voice Server. **Important:** Both the **B3.EnableAPSD** and **B3.EnableWMM** properties must be set to the same value.
EnableHandsetQuickEntry	Enables Easy Access entry to Privacy mode.
HandsetMode	Enables or disables Privacy mode using Easy Access.
HandsetQuickEntryPromptPlay	Plays an audible alert, “Entering Handset Mode” while switching to Privacy Mode using Easy Access.
B3.InstallDone	Specifies whether the Badge Properties Editor has performed the initial configuration for a badge: • **TRUE** specifies that the badge boots the normal Vocera application when it powers up. • **FALSE** specifies that the badge attempts to connect to a machine at IP address 10.0.0.1 running the Vocera Voice Server when it powers up. If successful, the badge downloads properties and firmware from the Vocera Voice Server.
B3.ListenInterval	An access point broadcasts a management frame called a beacon at a fixed interval (required to be set to 100 ms by Vocera). The **B3.ListenInterval** property specifies the frequency with which badges "wake up" and listen for a beacon. When the beacon interval is 100 ms and **B3.ListenInterval** is 5, the default listen interval is 500 ms.
B3.ResetVolumeToDefault	Specifies whether the badge resets the volume to the default at boot-up. • **FALSE** specifies that the badge maintains the previous volume setting at boot-up. • **TRUE** specifies that the badge resets the volume to the default at boot-up.
B3.SubnetMask	Specifies a subnet mask that indicates the bits in the IP address that correspond to the subnet, using standard dotted notation. For example: 255.255.255.0. You must specify this property if you are using static IP addresses. Leave this field blank if a DHCP server is assigning IP addresses.
B3.SubnetRoaming	Specifies whether users can roam across subnet boundaries while using badges. If subnet roaming is enabled, a badge automatically obtains a new IP address as a badge user makes the transition to an access point on a different subnet. If you enable subnet roaming, you must use a DHCP server to supply your IP addresses. **TRUE** specifies that the access points on your wireless LAN are divided into multiple subnets, and if you want to allow users to roam across subnet boundaries. **FALSE** specifies that all the access points on your wireless LAN are within a single subnet. Set this property to minimize DHCP traffic and reduce the chance of a momentary loss of audio when roaming between access points. The subnet where the Vocera Voice Server is located is not relevant to this property.

B3000N Badge Properties Configuration

This section lists the badge properties that you can configure using the BPE on your B3000N Badge.

Enter information or check the following badge properties:

Fields	Description
Profiles	
Selected Profiles	Specifies the name of the profile you selected to control general behavior. You must use the `profiles.txt` file for environments that require more than one wireless profile in a dynamic campus-type setting.
Create Profile	Allows you to create a new profile to control general behavior.
General Settings	
Server IP Address*	Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field. Use dotted-decimal notation to specify this value. For example, `192.168.3.7`. If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces. **Note:** Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.
SSID*	Specify an SSID other than vocera (all lower-case) for your production server. Badges are factory-programmed to use the vocera SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.
Hide Boot Menus	Specifies the option to prevent configuration menus to be displayed on a badge. The menus provide access to powerful utilities for maintenance and troubleshooting. Use these utilities only when you are working with Vocera Technical Support. **Note:** This property is ignored by the B3000 and B3000n badges, with menus always hidden.
Group Mode	Specifies the option to ensure noise-canceling microphones are turned off while users are on a call. Group Mode widens the speech zone, allowing additional people to speak into the primary microphone of the badge. Uncheck this option if you want to eliminate background noise when users are on a call. **Note:** B3000 and B3000n users can change the Group Mode setting on their badges, overriding the default. • For B3000: Group Mode is always off during Genie interactions and broadcasts. • For B3000n: Group Mode is automatically enabled when the badge is turned to a 105-degree angle to improve voice recognition.
Reset Volume to Default	Specifies the option to reset the default volume at boot-up. Otherwise, the previous volume setting is maintained at boot-up.
Display Bluetooth Settings	Check the **Display Bluetooth Settings** box to display the Bluetooth configuration menu on the badge.
Security Settings	
Enable FIPS	Specifies the option to enable the badge cryptographic security module to run in a secure mode that conforms with Federal Information Processing Standard (FIPS) 140-2. When **Enable FIPS** field is checked, it requires WPA2-PSK, WPA2-PEAP, or WPA2-TLS.
Authentication Type	

Fields	Description
Open	Specifies that your wireless network does not require authentication.
LEAP	Specifies that your wireless network implements the Cisco LEAP protocol for authentication.
Username and Password*	Enter appropriate values in the **Username** and **Password** fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication. If your network uses EAP-TLS authentication with external certificates (instead of the Vocera Manufacturer Certificates), enter a value for the **Username** field but not the **Password** field. Otherwise, skip both these fields. Each badge on a Vocera Voice Server must use the same username and password. The username format depends on the requirements set by the RADIUS authentication server. For example, when you use LEAP with Cisco ACS and Windows Active Directory, enter domain \ userid in the **Username** field, where domain is a Windows domain name and userid identifies the user. Other RADIUS servers may require the username only. The password value is case sensitive. You can use initial or embedded spaces in either of these values; trailing spaces cause an error message when the values are saved. The badge supports a maximum of 128 alphanumeric characters for the **Username** and 32 alphanumeric characters for the **Password**. In addition, the badge supports the following characters for LEAP passwords: `^ # ! * @ % & $` **Note:** If you are using EAP-FAST authentication and you change the username or password values, you must also generate a new PAC file. With manual PAC provisioning, you must generate a new PAC file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer. With automatic PAC provisioning, you must restore the factory settings on the badge and reconfigure it. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.
WPA-PSK	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication.
Pre shared Key	If Authentication Type is set to **WPA-PSK**, the pre-shared field appears. The pre-shared key that the badge supplies for authentication is a 64-character, hexadecimal value.
WPA-PEAP	Specifies that your wireless network uses the WiFi Protected Access Protected Extensible Authentication Protocol for authentication.
EAP-FAST	Specifies that your wireless network uses Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling for authentication. EAP-FAST authentication enables you to select between automatic or manual PAC provisioning.
Enable Auto-PAC	Specifies the option to enable automatic download of a PAC from the Cisco ACS, and the ACS periodically refreshes the PAC to ensure it does not expire. To take advantage of automatic PAC provisioning, you must configure badges correctly by setting Auto-PAC properties. If you enable manual PAC provisioning, you must create a `.pac` file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer.

Fields	Description
Provision Auto-PAC on Expire	Specifies the option to enable automatic provisioning of a new PAC when it expires. If this property is unchecked, a badge with an expired PAC displays the following message: "Expired or invalid PAC credentials." **Note:** This message appears only if a badge has been powered off or did not roam at all for a while and the master key and the retired master key on the Cisco ACS have expired. If this happens, the badge must to be reconfigured. To take advantage of this feature, you must also select EAP-FAST authentication.
Auto-PAC Provision Retry Count	Specifies the option to limit the number of times a badge attempts to retry retrieving a PAC from the Cisco ACS after the first attempt failed. For example, the badge attempts to retry retrieving a PAC due to wireless network problems. Select a number from 0 to 5. If a badge exceeds the retry count, it displays the following message: `Too many retries for Auto-PAC provisioning`. By default, this property is set to 0 (indicates no retries). To take advantage of this feature, you must also select EAP-FAST authentication.
EAP-TLS	Specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication. Check the **EAP-TLS** field to enable the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your self-signed certificates or obtain them from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS. Alternatively, uncheck this box to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Computer. Vocera Manufacturer Certificates use 2048-bit RSA keys that provide excellent security for enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server. For more information on security certificates, refer to Vocera Device Configuration Guide.
Use Custom EAP-TLS Certificates	Specifies the option to enable the badge to use custom EAP-TLS certificates rather than Vocera Manufacturer Certificates. If you use custom EAP-TLS certificates, you must generate your self-signed certificates or obtain it from a trusted Certificate Authority (CA). If you check this box, additional configuration is required. You must install client-side certificates on the Vocera Voice Server and the configuration computer, install the server-side certificates on your authentication server, configure your authentication server for EAP-TLS, and specify the **Username** and **Client Key Password** properties. Alternatively, uncheck this box to use the Vocera Manufacturer Certificates. Vocera badges are preconfigured with EAP-TLS client certificates that are automatically downloaded from the Vocera Voice Server or the Badge Configuration Computer. Vocera Manufacturer Certificates use 2048-bit RSA keys that provide excellent security for enterprise and conform to industry standards and NIST recommendations. If you decide to use Vocera Manufacturer Certificates on the badge, you still need to install Vocera Voice Server-side certificates on your authentication server. This property is available only when the **Authentication** property is set to EAP-TLS.
Encryption Type	The encryption types available are: • TKIP-WPA—Specifies your network uses TKIP as defined by WPA. • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2 Use hexadecimal characters to enter the key that the access point is using.

Fields	Description
Wireless Settings	
Wireless Band	Select the wireless bands used by the B3000n badge: • **ABGN**—Uses all 802.11 wireless bands (a, b, g, and n) at 2.4 GHz and 5 GHz. This is the default setting. • **AN**—Uses 802.11a and 802.11n wireless bands at 5 GHz. • **BGN**—Uses the 802.11b, 802.11g, and 802.11n wireless bands at 2.4 GHz. • **A**—Uses the 802.11a wireless band at 5 GHz. • **BG**—Uses the 802.11b and 802.11g wireless bands at 2.4 GHz.
2.4 GHz Channels	
Set to Defaults (1, 6, 11)	Specifies the option to force badges to scan the three non-overlapping 2.4 GHz channels of 1, 6, and 11.
Specify Channels	Specifies the option to specify up to four arbitrary channels to scan. If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select **Specify Channels** and enter the specific channel numbers in a comma-separated list. Ensure that you specify only channels that are supported for your locale.
CCKM	Check **CCKM** box if you want to enable Cisco Certified Key Management. CCKM is a form of fast roaming supported on Cisco access points and various routers. Using CCKM, Vocera devices can roam from one access point to another without any noticeable delay during reassociation. After the RADIUS authentication server initially authenticates a Vocera device, each access point on your network acts as a wireless domain service (WDS) and caches security credentials for CCKM-enabled client devices. When a Vocera device roams to a new access point, the WDS cache reduces the time it needs to reassociate. To take advantage of this feature, your access points must also support CCKM, and you must use either LEAP, WPA-PEAP, EAP-FAST, or EAP-TLS authentication.
OKC	Check the **OKC** box to enable authentication between multiple APs in a network when APs are under common administrative control.
802.11r	Check **802.11r** box to permit continuous connectivity for devices in motion. 802.11r addresses the fast roaming and fast BSS transitions.
FT over DS	Check **FT over DS** box to configure fast transition roaming over the DS (distribution system).
802.11d	Check **802.11d** box if you are in a country where systems that use other standards in the 802.11 family are not allowed to operate.
802.11k	Check **802.11k** to discover the best available access point.
802.11w	Check **802.11w** box to support protected management frames. The options available are: • Disable • Optional • Mandatory **Note:** It is difficult to troubleshoot security of encryption-related issues if the management frames are encrypted. So, you have the option to disable it or make it optional. Enable 802.11w for WPA2-PSK-SHA256 profile to work.
5 GHz Channels	
Set to Defaults (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165)	Specifies the option to force B3000n badges to scan 5 GHz channels of 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165.

Fields	Description
Specify Channels	Specifies the option to specify up to four arbitrary channels to scan. If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select **Specify Channels** and enter the specific channel numbers in a comma-separated list. Ensure that you specify only channels that are supported for your locale.
Roaming Policy	Specifies how quickly a badge searches for an access point when signal quality drops. Higher values cause a badge to search sooner and may correct problems with choppy audio. However, a badge cannot send or receive audio packets while searching for an access point, as communication may be interrupted. Lower values allow a badge to tolerate lower signal quality before searching. The optimal threshold value varies from one 802.11 network to another, depending on how the network is configured. Select a value from 1 to 5. The default value is 2.
Custom Settings	
B3N.BroadcastUsesIGMP	Vocera broadcast is implemented as IP Multicast. If broadcast commands need to cross a subnet, IGMP must be supported in the switch or router, and this property must be set to `TRUE`. The B3000n badge auto-detects IGMP and changes its mode dynamically if IGMP is enabled in the infrastructure. Consequently, this property is deprecated in the B3000n badge.
DefaultHandsetVolume	Lists the default volume level of Privacy Mode when no user is logged in.
DisplayHandsetMode	Displays Privacy Mode in the badge menu under Settings.
B3N.EnableAPSD	Specifies whether the badge takes advantage of the Unscheduled Automatic Power Save Delivery Subset (U-APSD) of 802.11e. U-APSD improves power management and potentially increases the talk time of 802.11 clients. • `FALSE` specifies that U-APSD is disabled. • `TRUE` specifies that U-APSD is enabled. To take advantage of this standard, your access points must also support it. **Important:** Both the `B3N.EnableAPSD` and `B3N.EnableWMM` properties must be set to the same value. The firmware and chip set changes in the B3000n badge make this property unnecessary. Consequently, this property is deprecated in the B3000n badge.
B3N.EnableWMM	Specifies whether the badge takes advantage of the WiFi Multimedia (WMM) subset of 802.11e. The 802.11e QoS prioritizes voice over data traffic and ensures high-level voice quality. • `FALSE` specifies that 802.11e QoS is disabled. • `TRUE` specifies that 802.11e QoS is enabled. To take advantage of this standard, your access points must also support it. Switches and routers must be configured to honor DSCP markings, and the Vocera QoS Manager service must be enabled on the Vocera Voice Server. If 802.11n is enabled on both the network and the B3000n badge (through the `B3N.WirelessBand` property), the B3000n takes advantage of WMM and ignores this property. In legacy 802.11n environments, you can continue to use this property for the B3000n badge. This property is not tied to the use of APSD for the B3000n.
EnableHandsetQuickEntry	Enables easy access entry to Privacy mode.
HandsetMode	Enables or disables Privacy mode using easy access.
HandsetQuickEntryPromptPlay	Plays an audible alert, `Entering Handset Mode` while switching to Privacy Mode using Easy Access.

Fields	Description
B3N.InstallDone	Specifies whether the Badge Properties Editor has performed the initial configuration for a badge: • `TRUE` specifies that the badge boots the normal Vocera application when it powers up. • `FALSE` specifies that the badge attempts to connect to a machine at IP address 10.0.0.1 running the Vocera Voice Server when it powers up. If successful, the badge downloads properties and firmware from the Vocera Voice Server.
B3N.ListenInterval	Specifies the frequency in which a badge "wakes up" and listen for a beacon. When the beacon interval is 100 ms and `B3.ListenInterval` is 5; the default listen interval is 500 ms. An access point broadcasts a management frame called a beacon at a fixed interval (required to be set to 100 ms by Vocera).
B3N.ResetVolumeToDefault	Specifies whether the badge resets the volume to the default at boot-up. • `FALSE` specifies that the badge maintains the previous volume setting at boot-up. • `TRUE` specifies that the badge resets the volume to the default at bootup.
B3N.SubnetMask	Specifies a subnet mask that indicates the bits in the IP address corresponds to the subnet, and uses standard dotted notation. For example 255.255.255.0. You must specify this property if you are using static IP addresses. Leave this field blank if a DHCP server assigns IP addresses.
B3N.SubnetRoaming	Specifies whether users can roam across subnet boundaries while using badges. If subnet roaming is enabled, a badge automatically obtains a new IP address when a user transitions to an access point on a different subnet. If you enable subnet roaming, you must use a DHCP server to supply your IP addresses. `TRUE` specifies that the access points on your wireless LAN are divided into multiple subnets and you want to allow users to roam across subnet boundaries. `FALSE` specifies that all the access points on your wireless LAN are within a single subnet. Set this property to minimize DHCP traffic and reduce the chance of a momentary loss of audio when roaming between access points. The subnet where the Vocera Voice Server is located is not relevant to this property.
B3N.ChannelstoScan	Specifies the list of channels to be scanned in 2.4GHz. Use this property to scan channels other than 1,6,11 mentioned in the specific channel options. If you do not specify channel numbers all the channels are automatically scanned.
B3N.ChannelstoScan5G	Specifies the list of channels to be scanned in 5GHz. Use this property to scan channels other than 1,6,11 mentioned in the specific channel options. If you do not specify channel numbers all the channels are automatically scanned.
B3N.HeadsetMicSupport	Specifies the option to enable or disable the headset mic when a 2.5 mm headphone is used. Set the value to `True` if the headset has a mic and `False` if it does not have a mic. The default value of the property is true. This property option can also be enabled/disabled from the Badge Settings.

V5000 Smartbadge Properties Configuration

This section lists the Smartbadge properties that you can configure using the BPE on your V5000 Smartbadge.

Enter information or check the following Smartbadge properties:

Fields	Description
Profiles	
Selected Profiles	Specifies the name of the profile you have selected to control general behavior. You must use the `profiles.txt` files for environments that require more than one wireless profile in a dynamic campus-type setting.
Create Profile	Allows you to create a new profile to control general behavior.
General Settings	
Server IP Address*	Specifies the IP address of the computer that runs the Vocera Voice Server. This is a required field. Use dotted-decimal notation to specify this value. For example, `192.168.3.7`. If you are configuring a cluster, enter the IP address of each machine in the cluster, separated by commas, with no spaces. **Note:** Do not enter more than four comma-separated IP addresses. The Vocera Voice Server supports a maximum of four cluster nodes.
SSID*	Specify an SSID other than vocera (all lower-case) for your production server. Badges are factory-programmed to use the vocera SSID to establish a wireless connection to the configuration computer that you have set up for your Vocera system.
Display Bluetooth Settings	Check the **Display Bluetooth Settings** box to display the Bluetooth configuration menu on the Smartbadge.
Security Settings	
Enable FIPS	Specifies the option to enable the badge cryptographic security module to run in a secure mode that conforms with Federal Information Processing Standard (FIPS) 140-2. When **Enable FIPS** field is checked, it requires WPA2-PSK, WPA2-PEAP, or WPA2-TLS.
Authentication Type	
Open	Specifies that your wireless network does not require authentication.
WPA-PSK	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol for authentication.
WPA-EAP	Specifies that your wireless network uses the Wiki Protected Access Extensible Authentication Protocol for authentication. If this authentication type is set, EAP method options appear.
FT-PSK	Specifies that your wireless network uses the Fast Transition Pre-Shared Key protocol for authentication.
FT-EAP	Specifies that your wireless network uses the Fast Transition Extensible Authentication Protocol for authentication. If this authentication type is set, EAP Method options appear.
WPA-PSK-SHA256	Specifies that your wireless network uses the WiFi Protected Access Pre-Shared Key protocol with SHA-256 cryptographic hash functions for authentication.
WPA-EAP-SHA256	Specifies that your wireless network uses the WiFi Protected Access Extensible Authentication Protocol with SHA-256 cryptographic hash functions for authentication.

Fields	Description
	If **Authentication Type** is set to WPA-PSK, FT-PSK, WPA-PSK-SHA256, and WPA-EAP-SHA256, the pre-shared field appears. The pre-shared key that the badge supplies for authentication is a 64-character, hexadecimal value.
EAP Method	
TLS	Specifies that your wireless network uses Extensible Authentication Protocol-Transport Layer Security for authentication.
PEAP	Specifies that your wireless network uses the WiFi Protected Access Protected Extensible Authentication Protocol for authentication. The provisioning fields displayed are: • PEAP V0 • PEAP V1
FAST	Specifies that your wireless network uses Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling for authentication. EAP-FAST authentication enables you to select between automatic or manual PAC provisioning. The provisioning fields displayed are: • Disabled/manual • Unauthenticated • Authenticated • Unauthenticated and Authenticated
LEAP	Specifies that your wireless network implements the Cisco LEAP protocol for authentication.
Encryption Type	The encryption type available is • AES-CCMP—Specifies your network uses AES-CCMP as defined by WPA2
Username and Password*	Enter appropriate values in the **Username** and **Password** fields if your network uses either LEAP, WPA-PEAP, or EAP-FAST authentication. If your network uses EAP-TLS authentication with external certificates (instead of the Vocera Manufacturer Certificates), enter a value for the **Username** field but not the **Password** field. Otherwise, skip both these fields. Each badge on a Vocera Voice Server must use the same username and password. The username format depends on the requirements set by the RADIUS authentication server. For example, when you use LEAP with Cisco ACS and Windows Active Directory, enter domain \ userid in the **Username** field, where domain is a Windows domain name and userid identifies the user. Other RADIUS servers may require the username only. The password value is case sensitive. You can use initial or embedded spaces in either of these values; trailing spaces cause an error message when the values are saved. The badge supports a maximum of 128 alphanumeric characters for the **Username** and 32 alphanumeric characters for the **Password**. In addition, the badge supports the following characters for LEAP passwords: `^ # ! * @ % & $` **Note:** If you are using EAP-FAST authentication and you change the username or password values, you must also generate a new PAC file. With manual PAC provisioning, you must generate a new PAC file on the Cisco ACS and copy it to the Vocera Voice Server and the Vocera configuration computer. With automatic PAC provisioning, you must restore the factory settings on the badge and reconfigure it. When the badge reconnects, it retrieves the new PAC file automatically from the ACS.
Wireless Settings	
Wireless Band	Select the wireless bands used by the V5000 Smartbadge:

Fields	Description
	• **ABG**—Uses all 802.11 wireless bands (a, b, and g) at 2.4 GHz and 5 GHz. This is the default setting. • **A**—Uses the 802.11a wireless band at 5 GHz. • **BG**—Uses the 802.11b and 802.11g wireless bands at 2.4 GHz. **Note:** 802.11n and 802.11ac are enabled by default on the Vocera device. If the infrastructure does not support 802.11n or 802.11ac, the device radio automatically falls back to use legacy 802.11abg protocol.
2.4 GHz Channels	
Set to Defaults (1, 6, 11)	Specifies the option to force badges to scan the three non-overlapping 2.4 GHz channels of 1, 6, and 11.
Specify Channels	Specifies the option to specify up to four arbitrary channels to scan. If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select **Specify Channels** and enter the specific channel numbers in a comma-separated list. Ensure that you specify only channels that are supported for your locale.
802.11d	Check **802.11d** box if you are in a country where systems that use other standards in the 802.11 family are not allowed to operate.
802.11k	Check **802.11k** box to discover the best available access point. Vocera recommends enabling this option to advertise channels of both the bands.
OKC	Check the **OKC** box to enable authentication between multiple APs in a network when APs are under common administrative control.
802.11w	Check **802.11w** box to support protected management frames. The options available are: • Disable • Optional • Mandatory **Note:** It is difficult to troubleshoot security of encryption-related issues if the management frames are encrypted. So, you have the option to disable it or make it optional. Enable 802.11w for WPA2-PSK-SHA256 profile to work.
5 GHz Channels	
Set to Defaults (36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165)	Specifies the option to force V5000 Smartbadges to scan 5 GHz channels of 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165.
Specify Channels	Specifies the option to specify up to four arbitrary channels to scan. If the access points on your network are set either to four channels, three channels, or to fewer than three channels other than 1, 6, and 11, select **Specify Channels** and enter the specific channel numbers in a comma-separated list. Ensure that you specify only channels that are supported for your locale.
Roaming Policy	Specifies how quickly a badge searches for an access point when signal quality drops. Higher values cause a badge to search sooner and may correct problems with choppy audio. However, a badge cannot send or receive audio packets while searching for an access point, as communication may be interrupted. Lower values allow a badge to tolerate lower signal quality before searching. The optimal threshold value varies from one 802.11 network to another, depending on how the network is configured. Select a value from 1 to 5. The default value is 3.
Custom Settings	

Fields	Description
V5.EnableConsoleLog	Specifies the option to enable or disable console log. Set the value to `FALSE`.
V5.MinimumVolume [0-6]	Specifies the option to enable volume to be set to 0 for all incoming calls, pages, alerts, and messages.
V5.EventDisplayActivate	Specifies the option to activate display notification based on incoming events. If the "Raise to Wake" option is also enabled on your Smartbadge, the badge property `V5.EventDisplayActivate` directly opens the notification. The default value of the property is `true`.
V5.EnableHotwordLedIndication	Specifies the option to enable or disable LED indication when hotword detection is active, and the screen is turned off. Set the value to `TRUE` to enable LED indication. Set the value to `FALSE` to disable LED indication.
V5.ForceIGMPVersion	Specifies the option for the Smartbadge to negotiate IGMP version to be used in the network. Default version is 3 and is backward compatible with version 1 and version 2.
v5._EnableDigitalHS_	Specifies the option for the Smartbadge to detect or not detect the USB-C Digital headset. The default value is false. Analog headsets continue to work as before regardless of the digital headset property.
V5.EnableHotword	Specifies the option to enable the voice command "OK Vocera" to initiate a Genie call. When the option is enabled, the V5000 Smartbadge listens for a spoken phrase. When that phrase is detected, the V5000 initiates a call to the Genie. The default value of the property is `false`.
V5.DirectCallEnabled	Specifies the option to enable direct calling. Set the value to true to enable direct calling. The default value of the property is `false`.
V5.ChannelsToScan	Specifies the list of channels to be scanned in 2.4GHz and 5GHz band together. Use this property to specify scan channels. If you do not specify channel numbers all the channels are automatically scanned. Vocera recommends using this badge property for scanning. For example: 36, 40, 44, 48, 149, 153, 157, 161, and 165.
V5.EnableAutoHandsetModeFt	Specifies the option to expose automatic handset mode. You can enable or disable automatic handset mode from the badge settings menu if the feature is enabled using the badge property. The option is set after the call is established and is active only when the badge is in the regular speaker mode. This feature is disabled for headset mode. If you take the device away from the ear during the call, the call remains in handset mode. You can use the screen options to change back to the handsfree mode when needed. The device returns to the handsfree mode after the call ends.
V5.UseSHA2cert	Specifies the option to switch between the SHA1 certificate and the new Vocera SHA2-256 certificate with 2048 bit RSA encryption. The default value is `V5.UseSHA2cert` is `true`.

Configuration Packages

The EMDAN solution includes configuration packages providing components that most typical Vocera Platform health care customers need. When these packages are installed, they deploy the dataset conditions, rules, adapters, templates, templated events, and workflows needed to support typical health care functionality.

The EMDAN solution comprises two sets of packages:

- Core packages
- Supplementary packages

The core configuration package contains all dataset conditions that are not solely used by a supplemental package, all roles, and a number of adapters and workflows. The supplemental packages contain the dataset conditions, workflows, and adapters to enable functionality needed for a particular implementation, such as Alarm Notification or Basic Assignment.

Use the information provided in this section of the Vocera Platform Administration Guide to install the Vocera EMDAN solution configuration packages, which include the core solution configuration package, as well as the supplemental solution configuration packages for additional specific functionality.

In this installation process, you will upload the core solution configuration package as an XML file, any additional XML packages required for the implementation, and make configuration edits to adapters as required for the implementation. See an Administrator for additional information if needed.

About the Core Configuration Packages

The two core packages (engage-2.1.0.99.xml and alarm_notification-2.1.0.99.xml) allow you to configure the basic functionality of the Vocera Platform, such as the XMPP and CUCM adapters. These packages are needed by all customers.

Following are the adapters and workflows provided by installing the engage-2.1.0.99.xml package:

Adapters	Workflows
ComplianceLogger	AdminMenu
CUCM	AlertsClinicals
CustomAudit for CUCM	AlertsDM
DataUpdate for Alerts	AlertsEvents
DataUpdate for Facility Setup	AlertsLabs
DataUpdate for XMPP	AlertsList
HL7 ADT	AlertsMT
HL7 Lab Tests	AlertsNCM
HL7 Orders	AlertsNurseCalls
HL7 Reports	AlertsOrders
LDAP	AlertsReports
Media	AssignmentCurrentUserToDevice
NurseCalls	AssignmentUserToDevice
XMPP	AssignmentWebUserToDevice
	AssignmentWebUserToDeviceAdmin
	AssignUserGroups
	DeliveryTracking
	Directory
	Help
	ManageConfiguration
	ManageDevices
	ManageFunctionalRoles
	ManageLocations
	ManageMonitorAssignments
	ManageMonitorTech
	ManageMyMessageFavoritesPhone
	ManageMyQuickResponseFavoritesWeb
	ManagePresenceStates
	ManageQuickResponses
	ManageUserPresence
	Patients
	PatientsFromPhone
	PatientsUnitOnly
	SendGrp
	SendMessage
	SendWebMessage
	TrackAlerts
	TrackDMs
	TrackDMsFromPhone
	TrackDMsUserOnly
	ViewEngageStaffAssignment
	ViewRegistrationHistory
	ViewRoleStaffAssignment
	ViewStaffAssignmentHistory

Following are the adapters and workflows provided by installing the alarm_notification-2.1.0.99.xml package:

Adapters	Workflows
AlarmNotification	N/A

About the Supplementary Configuration Packages

The supplementary packages allow you to configure functionality that is specific to typical health care environments, such as adapters that connect the Vocera Platform to common clinical systems and the Staff Assignment feature in the browser and Vina.

Only install a supplemental package if it is required by your implementation. If a supplemental package is required, install it after the core solution configuration package is installed on the Vocera Platform.

Once a supplemental package is installed, add any associated workflows in the Vocera Platform Web Console. If a workflow is implemented in a supplemental package, such as a staff assignment workflow, you must add the link in the Vocera Platform Web Console to enable users to access the workflow.

The following supplementary packages are designed for use with the core EMDAN solution configuration packages:

Supplementary Package	Adapter	Workflow	Condition
ascom-2.1.0.99.xml	Ascom		Contains conditions related to Ascom devices on the datasets Clinicals, DM, NurseCallMessages, and NurseCalls.
basic_assignment-2.1.0.9	DataUpdate for Basic Assignment	AssignmentBasic	Contains a few conditions related to basic assignments on the datasets Assignments and Locations.
epic_treatment_team-2.1.	AssignmentManager HL7 Epic ADT		Contains conditions related to managing assignments on the dataset Assignments.
outgoingwctp-2.1.0.99.xm	OutgoingWCTP		Contains conditions related to WCTP devices on the datasets Clinicals, DM, LabTests, NurseCallMessages, NurseCalls, Orders, and Reports.
responder_sync-2.1.0.99.x	CustomAudit for ResponderSync DataUpdate for Functional Roles ResponderSync		Contains a condition related to managing the location of an assignment on the datasets Assignments and ContactDetails.
spacelabs-2.1.0.99.xml	Spacelabs CEI		
spectralinkxml-2.1.0.99.x	CustomAudit for SpectraLinkXML SpectraLinkXML		Contains conditions related to SpectraLinkXML devices on the datasets Deliveries, Clinicals, DM, LabTests, NurseCallMessages, NurseCalls, Orders, and Reports.
staff_assignment-2.1.0.99		AssignmentClerk AssignmentPhone ViewAssignmentPhone	Contains conditions related to staff assignment on the datasets Assignments, Locations, Groups, Units, Users
vmp-2.1.0.99.xml	DataUpdate for VMP Patient Context VMP		Contains conditions related to SpectraLinkXML devices on the datasets Deliveries, Clinicals, LabTests, NurseCallMessages, NurseCalls, Orders, and Reports.
vocera_messaging_interfa	DataUpdate for Vocera Messaging Interface		Contains conditions related to Vocera Messaging Interface on the datasets DeliveryHistory, Responses, Clinicals, LabTests, NurseCallMessages, NurseCalls, Orders, and Reports.

Working with Configuration Packages

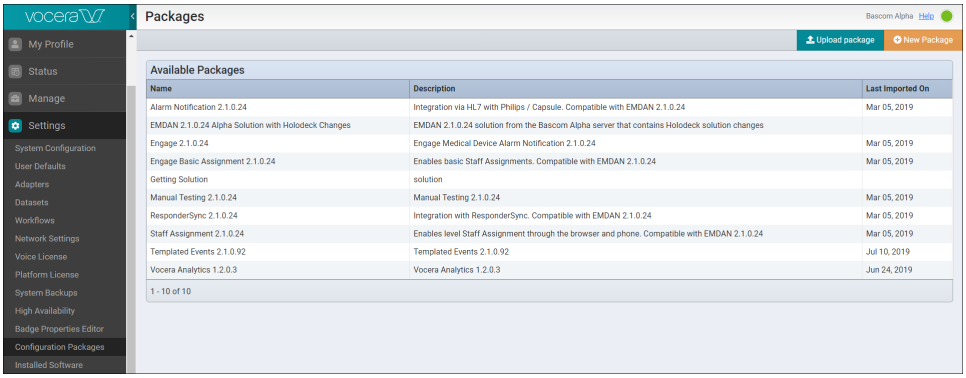
Use the **Packages** home page to manually upload, install, or remove packages, and to perform other manual operations with configuration packages.

When you install the Vocera EMDAN solution at the command line, the configuration files associated with your Vocera license are automatically retrieved and imported.

After you install the solution, you can manage the packages that you have imported (for example, you can update them or remove them) through the **Configuration Packages** user interface. If necessary, you can also import additional packages through this UI.

Important: Install the core solution configuration package only once; do not attempt to install a new solution over an older one again through the command line.

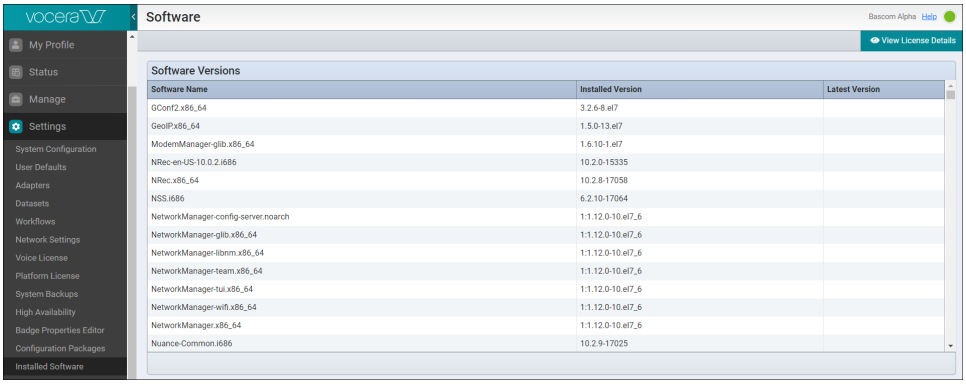
To view the **Pacakges** home page, navigate to **Configuration Packages** in the **Settings** section of the menus.



Installed Software

After your installation is complete, use the **Installed Software** page to see the full list of software that is installed on your system.

To view the **Installed Software** home page, navigate to **Installed Software** in the **Settings** section of the menus.



The **Installed Software** page displays the following information:

Field	Description
Software Name	The name of the software component installed on your system. Names that begin with "vocera", "voice-server", and "extension" identify components developed by Vocera. Other names are typically open source 3rd-party components, or components provided by Red Hat.
Installed Version	The version number of the software component.
Latest Version	The number of most recent version found in Vocera's repository; if no value appears in this column, you have the most recent version. When a version number appears in this column, that version of the component has been tested and approved by Vocera; you may optionally contact Vocera Customer Support to determine if you should upgrade that component.

Use the **View License Details** button in the Action bar to display information about your platform license. This button is a shortcut to the **Platform** page. See Platform License on page 331 for information about the content of this page.

Security

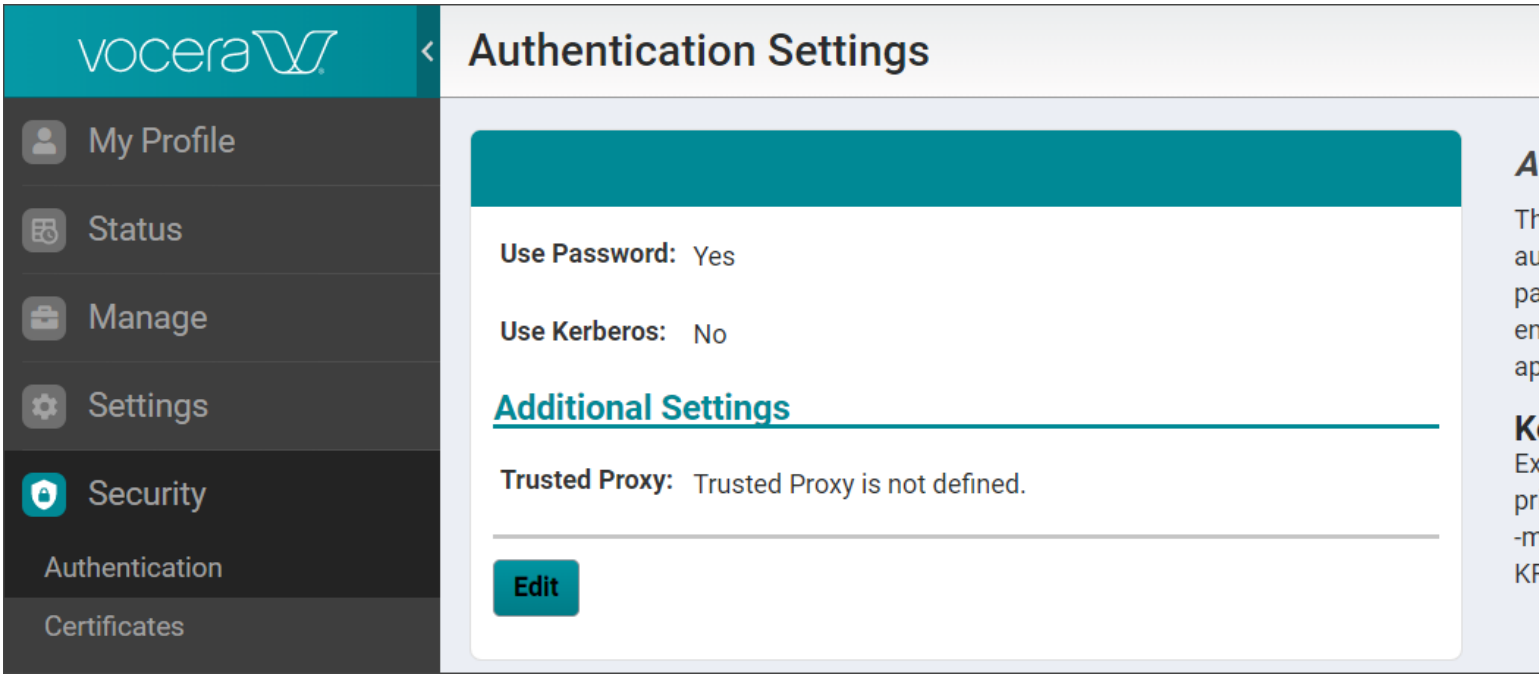
The **Security** section of the **navigation bar** in the Vocera Platform Web Console allows you to establish and maintain system security.

- Authentication on page 390
- Certificates on page 397
- Security Policies on page 399
- Roles on page 417
- Remote Support on page 423

Authentication

You can add, configure, and enable/disable authentication methods you choose for your system.

The **Authentication Settings** in the Vocera Platform Web Console provide configurable options for managing system access. A System Administrator can configure Password or Kerberos authentication methods for authenticating users to access the Vocera Platform. They can also configure the system to handle proxied requests in a clustered environment that utilizes an application delivery controller (ADC) such as BIG-IP.

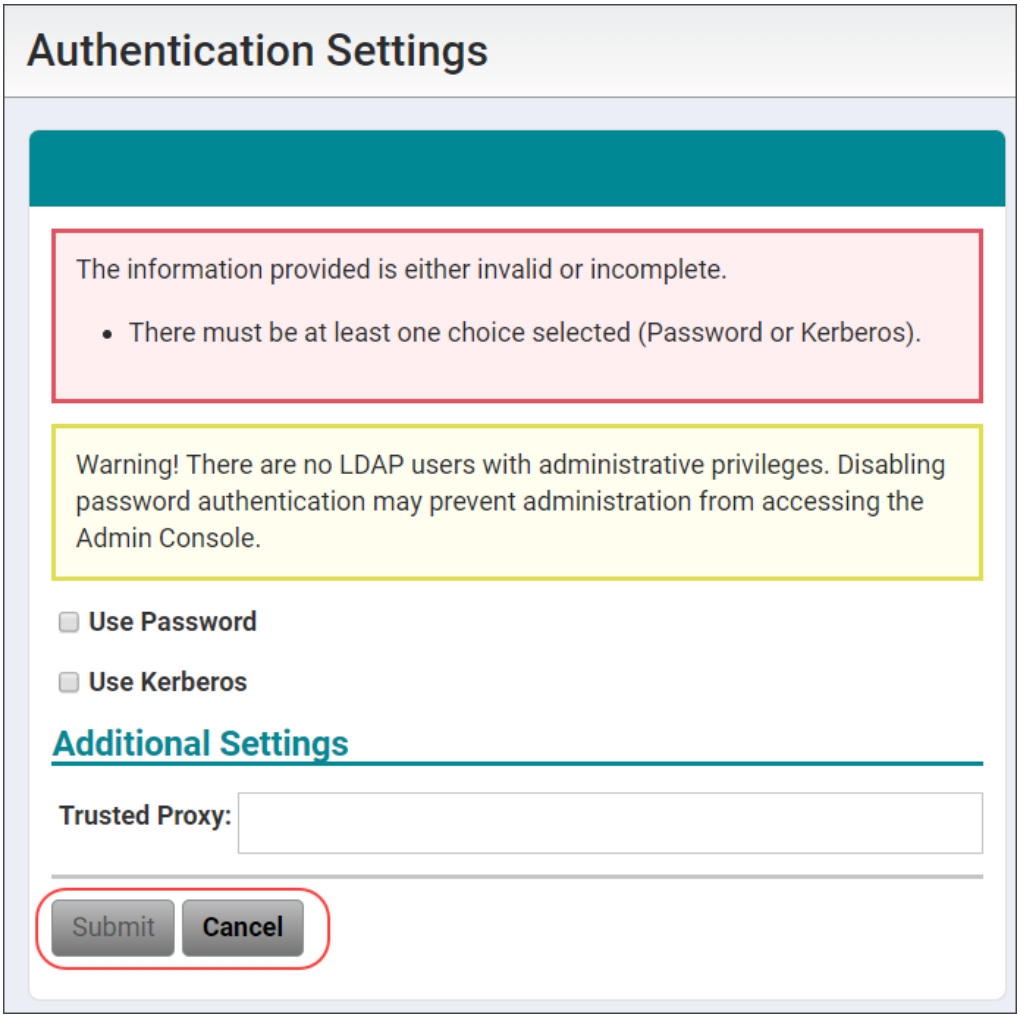


Password authentication allows users to access the Vocera Platform with a password. This option is enabled by default in the Authentication Settings configuration.

Kerberos is a network authentication protocol implemented in the user's facility to authenticate user accounts in the system. This option provides strong authentication for client/server applications by using secret-key cryptography. Kerberos authentication is disabled by default, and can be enabled in Authentication Settings. A System Administrator can use the Kerberos authentication method to upload keytab files for server credentials and set the allowed Kerberos realms for authenticating clients to the HTTP service.

When both Password and Kerberos methods are selected in the Vocera Platform Web Console, and the user is unable to authenticate via Kerberos, they can still be authenticated via a password. The Windows domain authentication supports Kerberos; when Kerberos is properly configured, Windows integrated authentication works with the Vocera Platform Web Console.

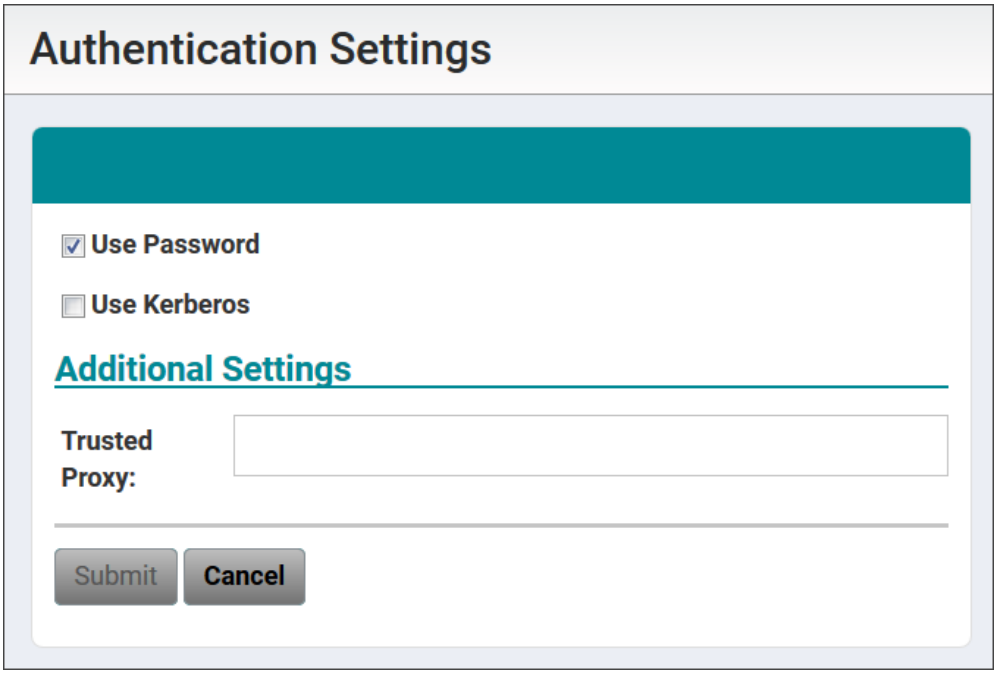
At least one authentication method must be selected. The configuration edits cannot be saved if both options are unselected. In this example where neither authentication method is selected, the Submit option is not active, which prevents a user accidentally putting the system into a state where it cannot be accessed.



Configuring Authentication Settings

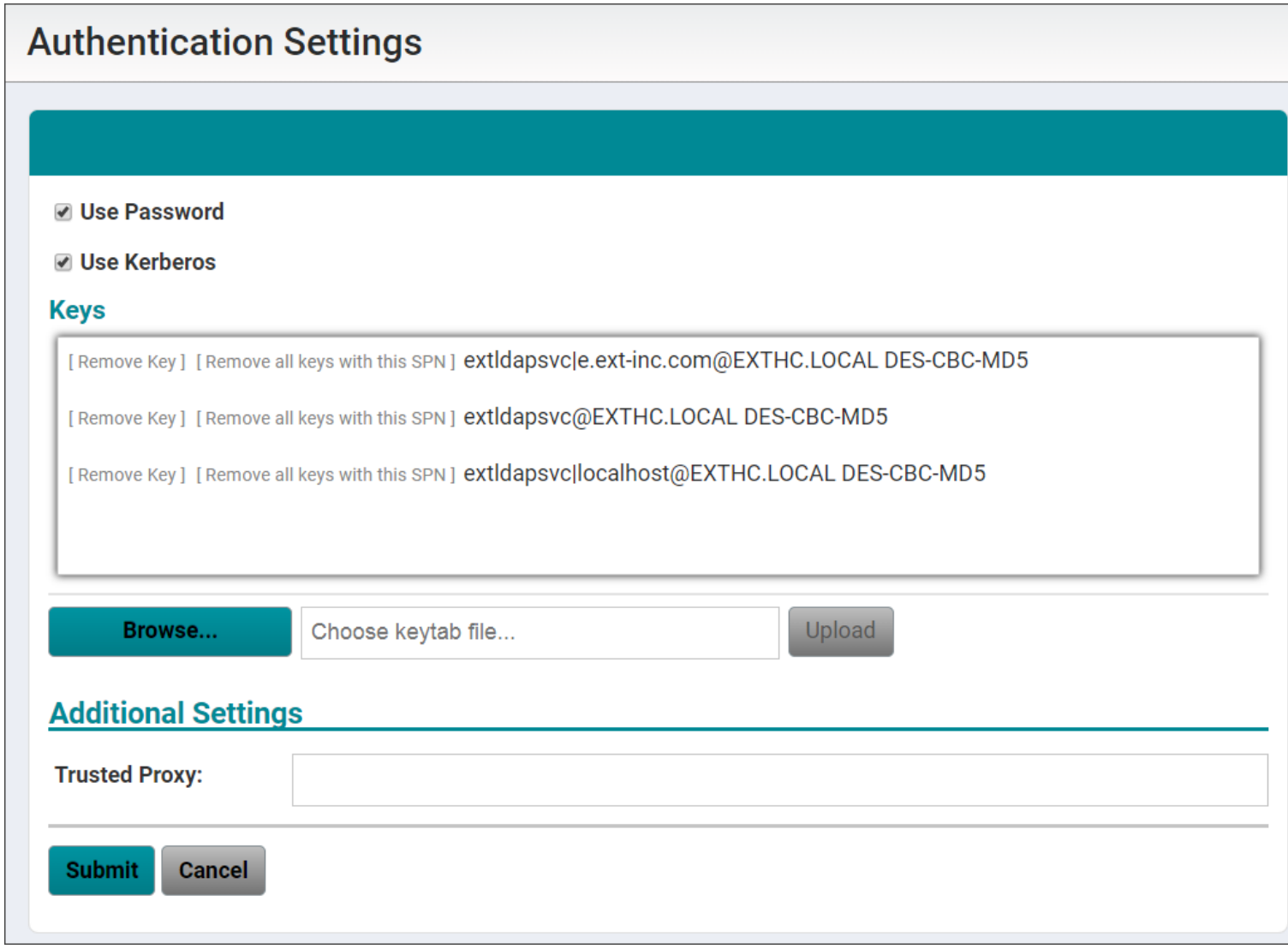
Configure Password or Kerberos authentication, and enable secure (https) connection through the Vocera Platform Web Console.

1. Navigate to **Authentication** in the Security section of the Vocera Platform Web Console.
   The Authentication Settings page appears.
2. Select **Edit** in the Authentication Settings page.
   The configuration fields for Authentication Settings display.
3. Complete the **Authentication Settings** configuration fields using the information described in the following table.



Configuration	Description
Use Password	Select the **Use Password** checkbox to allow an account password to be used as the authentication method for user access to the Vocera system. This option can be enabled or disabled. Before disabling this option, ensure that at least one role has the Advanced Support policy, or an LDAP user is assigned a role with the Advanced Support policy. When no authentication method is selected, the following warning displays: **Warning:** There are no LDAP users with administrative privileges. Disabling password authentication may prevent administration from accessing the Vocera Platform Web Console.
Use Kerberos	Select the **Use Kerberos** checkbox to use this protocol to authenticate user's access to the Vocera system. Select Use Kerberos to display the Keys configuration field. A message displays to remind you to upload a keytab file.
Keys	Select **Browse** and locate the Kerberos keytab file to apply, then select **Upload**. Review the uploaded keytab entries displayed in the Keys list.
Trusted Proxy	Enter the IP address for a **Trusted Proxy**. In a clustered environment when the trusted proxy utilizes an application delivery controller (ADC), such as F5 BIG-IP or Citrix Netscaler, the system must be configured to handle proxied requests made by a trusted proxy. By default, incoming requests with the proxy's source IP are rejected. Enter the trusted proxy information in the Authentication Settings to allow the proxy IP to be replaced with the remote client IP of a HTTP workflow device, such as CUCM.

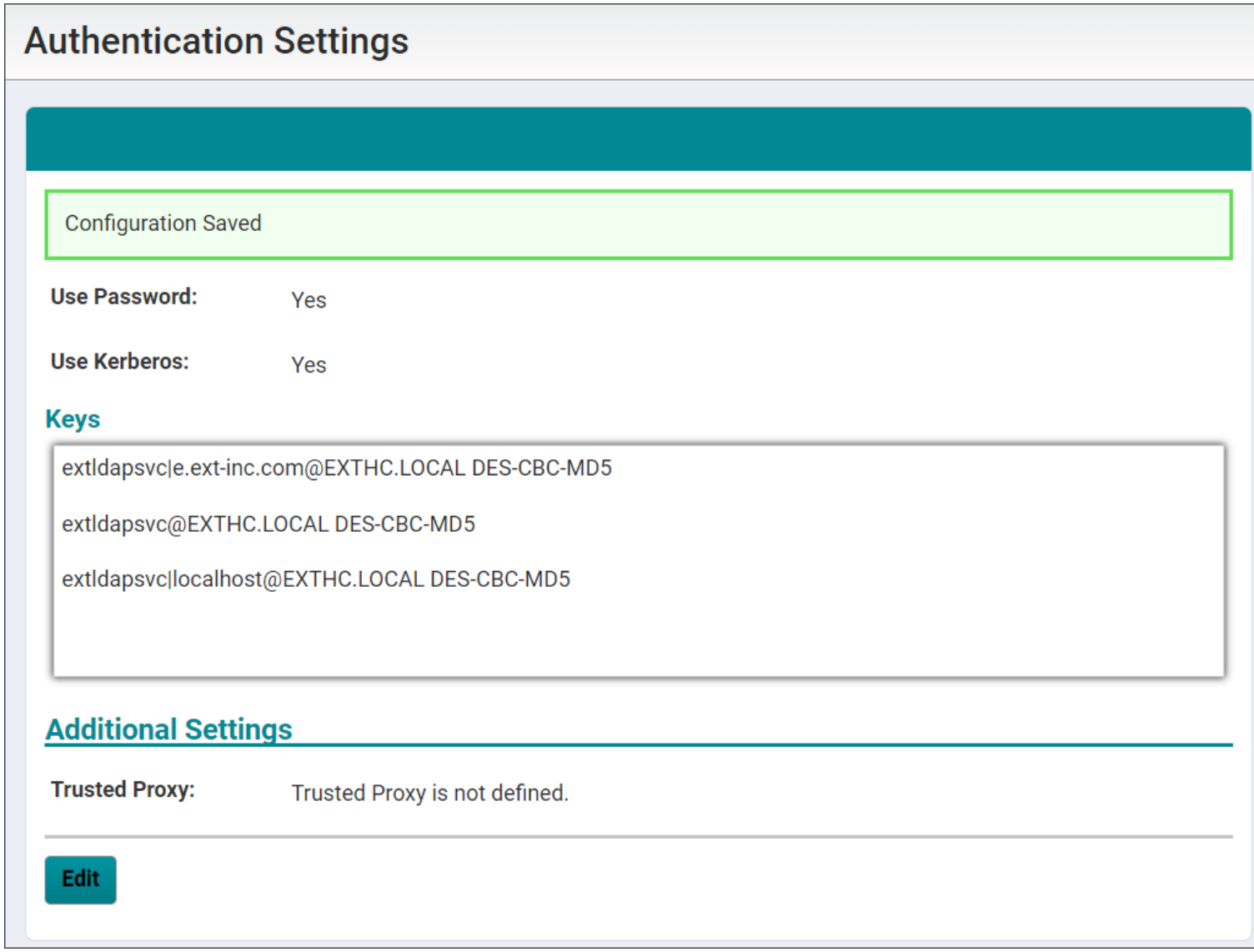
4. (Optional) Select **Use Kerberos** authentication. Browse to a stored keytab file and click **Upload**. See Using a Keytab File for Kerberos Authentication on page 394 for details on generating a keytab file.



The Keys section displays the uploaded keytab details.

5. Select one of the following to exit the **Authentication Settings** configuration:
   - Select **Submit** to save your changes to Authentication Settings.
   - Select **Cancel** to exit without making changes to the authentication configuration.

A message indicates the configuration success or failure.



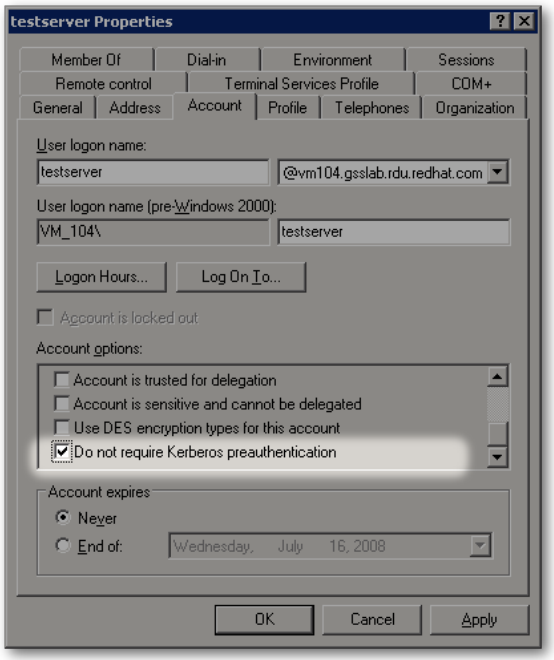
Using a Keytab File for Kerberos Authentication

A System Administrator can create the Kerberos keytab files used to authenticate user accounts in the Vocera system.

When Kerberos authentication is enabled, you can upload a keytab file provided by a Windows administrator to authenticate clients from multiple realms to the HTTP service. The keytab files are generated on the user's Active Directory server.
A **Vocera LDAP Adapter** is required for Kerberos keytab generation. For information on the LDAP adapter configuration, refer to the Vocera Adapters documentation section in the Vocera Documentation Portal.

Before generating the keytab file for Kerberos authentication, the System Administrator must:

- Obtain the domain name of the Vocera Platform cluster, and the name of a user account in Active Directory that represents the Vocera Platform.
- Ensure that Kerberos is configured and working correctly on the user's network. This configuration requires a service or computer account for the host and an HTTP principal entry for that host, with a keytab file containing a token for the HTTP principal placed on the Vocera Platform.
- Ensure that the computer's time is synchronized with the Active Directory server; Vocera recommends NTP setup for the Vocera Platform to ensure the time is synchronized. For instructions to Configure Microsoft Active Directory, refer to the RedHat website.
- Ensure that the Windows user account does not have "Do not require Kerberos preauthorization" checked. In this example the box is checked; be sure to uncheck this checkbox.



To generate a keytab file:

1. Issue the `ktpass` command to map the trusted host and generate the keytab file. The following parameters are used in the command. The principal and domain name case must match the case of the incoming request.

Commands	Description
`/out <FileName>`	Specifies the name of the Kerberos version 5 .keytab file to generate. This is the `.keytab` file that you upload in the Vocera Platform Web Console on the Vocera Platform.
`/princ <PrincipalName>`	Specifies the service principal name that is being mapped to, in the form '`host/computer.contoso.com@CONTOSO.COM`'. This parameter is case sensitive. Example: `HTTP/<FQDN of computer>@<domain name>`

Commands	Description
`/mapuser <UserAccount>`	Maps the name of the Kerberos principal user account being mapped to, which is specified by the **princ** parameter, to the specified domain account. Example: `<domain>\<user> -crypto All -pass <pass goes here> -ptype KRB5_NT_PRINCIPAL`

2. On the Active Directory server, substituting the user's details in the placeholders, enter the following command line:

   ```
   ktpass -princ HTTP/<FQDN of computer>@<domain name> -mapuser <domain>\<user> -crypto All -pass <pass goes here> -ptype KRB5_NT_PRINCIPAL -out <filename>.keytab
   ```

3. Store the resulting keytab file on the Vocera system for upload in Authentication Settings through the Vocera Platform Web Console.
4. (Optional) Instead of creating and uploading a separate file for each user as described in step 2, you can add multiple users to an existing single keytab file. Enter the `ktpass -princ` command for each distinct '-mapuser' value that you need to upload in the keytab file.

   ```
   ktpass -princ HTTP/testserver@kerberos.jboss.org -mapuser KERBEROS1\testserver -pass * -in C:\testeserver.host.keytab -out C:\testeserver.host.keytab
   ```

See Configuring Authentication Settings on page 391 for information on uploading the generated keytab file to the Vocera Platform.

Certificates

The Certificates feature in the Vocera Platform Web Console enables a System Administrator to implement Secure Sockets Layer (SSL) protocol security for Internet communication.

Communication that passes through a public network is susceptible to surveillance as well as manipulation. Vocera is committed to ensuring communication traveling over the Internet is kept confidential and secure.

Secure Sockets Layer (SSL) is a cryptographic protocol that provides communication security over the Internet. An SSL certificate is a digital certificate issued to a server (or domain, such as *.vocera.com) by a trusted certification service known as a Certification Authority (CA).

SSL certificates are used to validate the identity of the server, and possibly the client. The certificate verifies the organization's identity so that the client can securely connect to the server. This secure connection verifies that the server belongs to the identified organization, and that the communication between the server and client is encrypted.

A Certification Authority (CA) is an authority that issues SSL certificates. A CA certifies the ownership of a SSL certificate to it's organization. The CA acts as a trusted third-party, responsible to both the certificate's owner and the client relying upon the certificate. SSL certificates can be purchased from a CA (such as VeriSign, DigiCert, or Go Daddy), or an organization may have their own "Internal" Certificate Authority to manage SSL certificates.

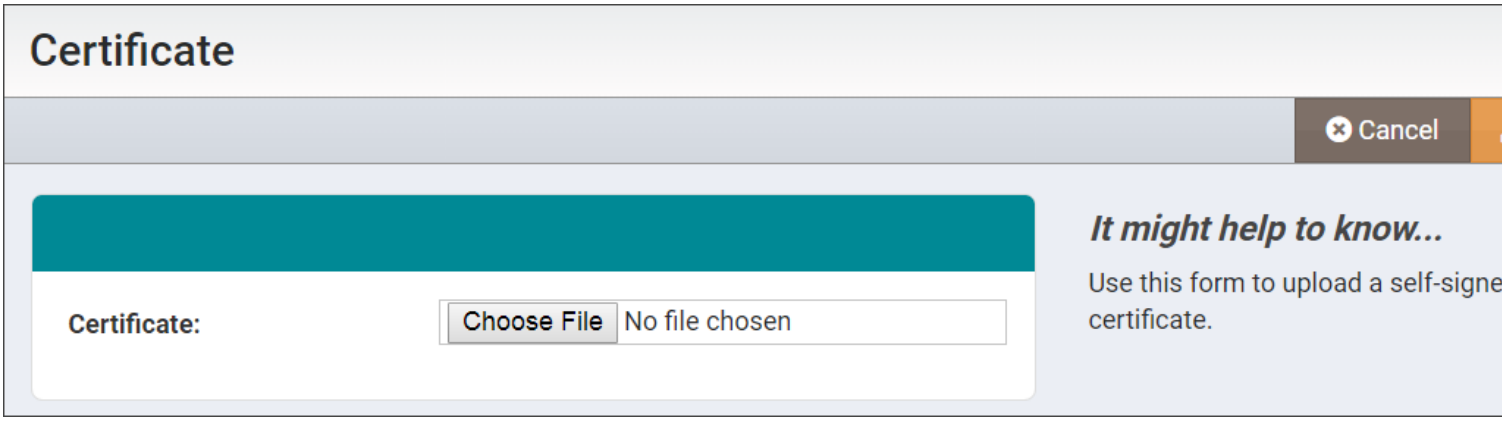
There are a few different categories of certificates available.

- Self-signed Certificates: Used for testing purposes. Not secure, not recommended in "production" environments. Using "out of box" SSL for Voice Server is self-signed.
- Internal CA Signed Certificate: An SSL Certificate that has been signed by an Internal Certificate Authority within the organization. Used where a Public Key Infrastructure (PKI) is deployed on a organization's network. Some Internal Certificate Authorities will be backed by a Public Signed Certificate.
- Public Signed Certificate: An SSL Certificate that has been signed by a Trusted Third Party organization who validates the organization's identity. These are recommended when access is made outside of the organization's network.

Uploading a Certificate

Navigate to a stored security certificate, and upload it to the Vocera system.

1. Navigate to **Certificates** in the Security section of the Vocera Platform Web Console.
   The Certificate page appears.
2. Navigate to the stored certificate file and display it in the **Choose File** field in the Certificate page.



3. Select one of the following menu options to leave the Certificate page.
   - Select **Cancel** to exit the page without making a change.
   - Select **Upload Certificate** to load the selected certificate to the Vocera system.

Security Policies

Security policies enforce rules that control the user access and authentication features on the Vocera system.

System administrators can create security policies and associate them with a variety of policy items to ensure that users have access and authentication privileges when accessing the Vocera system via the Vocera Platform Web Console, mobile clients, or supported Vocera devices.

You can create multiple security policies with a variety of security policy items as needed. You can also update an existing security policy with additional items to configure appropriate security settings for users. After creating policies, system administrators can associate the policies with a role. Roles determine whether users have permissions to access Vocera features. For more information on how roles work, see Roles on page 417.

As a system default, a Default Security Policy is applied to all users in the system. You cannot remove the default security policy; however, a user with appropriate permission can edit the name and description of a default security policy.

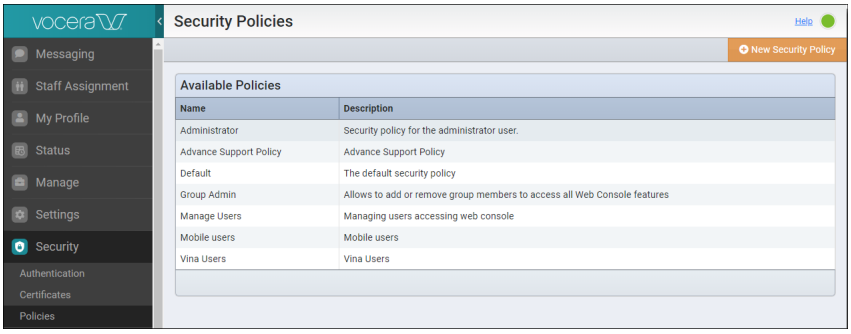
Accessing Security Policies

Establish and revise security policies designed to allow users controlled access to the Vocera system.

System administrators can create, edit, and remove the security policies from the Vocera system to meet the needs of their organization. Security policy items are added to a security policy to create a specific security access scenario. A user with the administrator role can manage security policies and security items for the entire facility.

A Default Security Policy is applied to all users in the system. The default security policy cannot be removed. A user with the appropriate permissions can edit the name and description of a policy.

To access security policies in the Web Console, select **Policies** in the **Security** section of the navigation bar.



From the Security Policies page, you can create, edit, view, and remove security policies and associated policy items.

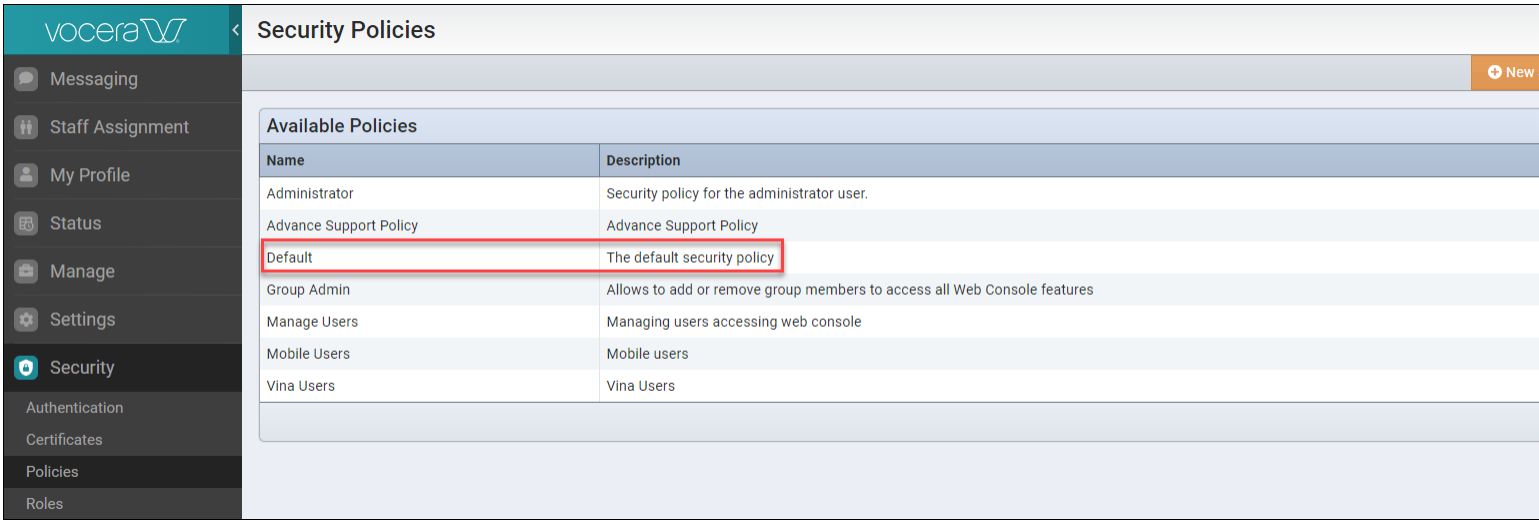
Default Security Policy

Vocera system creates the Default Security Policy at the time of installation, and this policy applies to all users in the system.

You cannot remove a default policy or change the name and description of the default security policy. However, you can view the name, description, and security policy items associated with the default security policy.

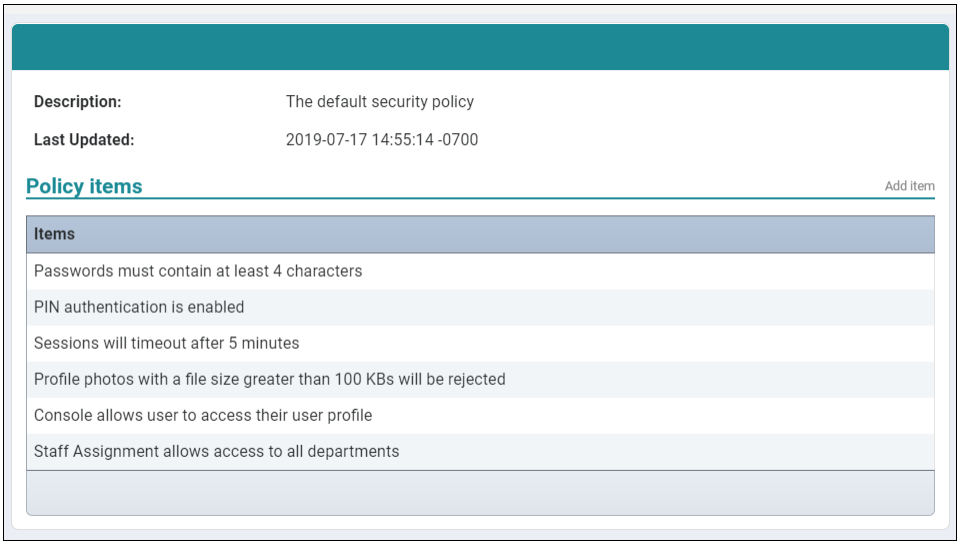
Remember: Each role in your system must have at least one security policy associated with it. If a user is a member of a group that's assigned a role with a customized security policy, the user will have access privileges and permissions based on both the customized policy and the default policy.

To view the default security policy items, select the **Default** security policy in the Security Policies page.



You can also add additional policy items to the default security policy.

For example, the following screenshot shows a list of security policy items included in the Default Security Policy.

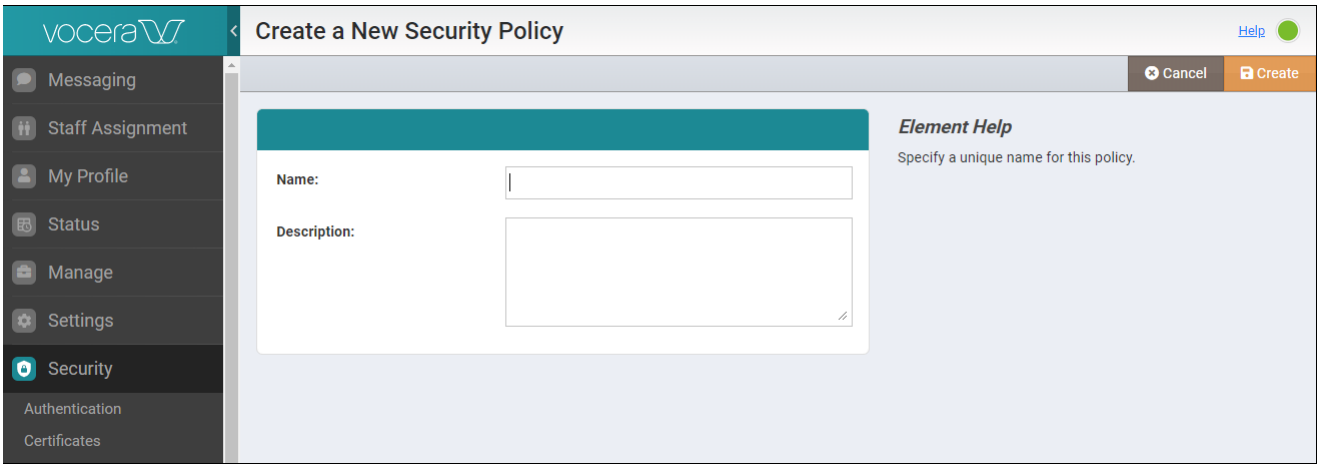


For more information on adding a polity item, see Adding a Policy Item on page 413.

Creating a Security Policy

A system administrator can create a customized security policy and assign this policy to a role or multiple roles.

1. Navigate to **Policies** in the **Security** section, and click **New Security Policy**.
   The **Create a New Security Policy** page displays.

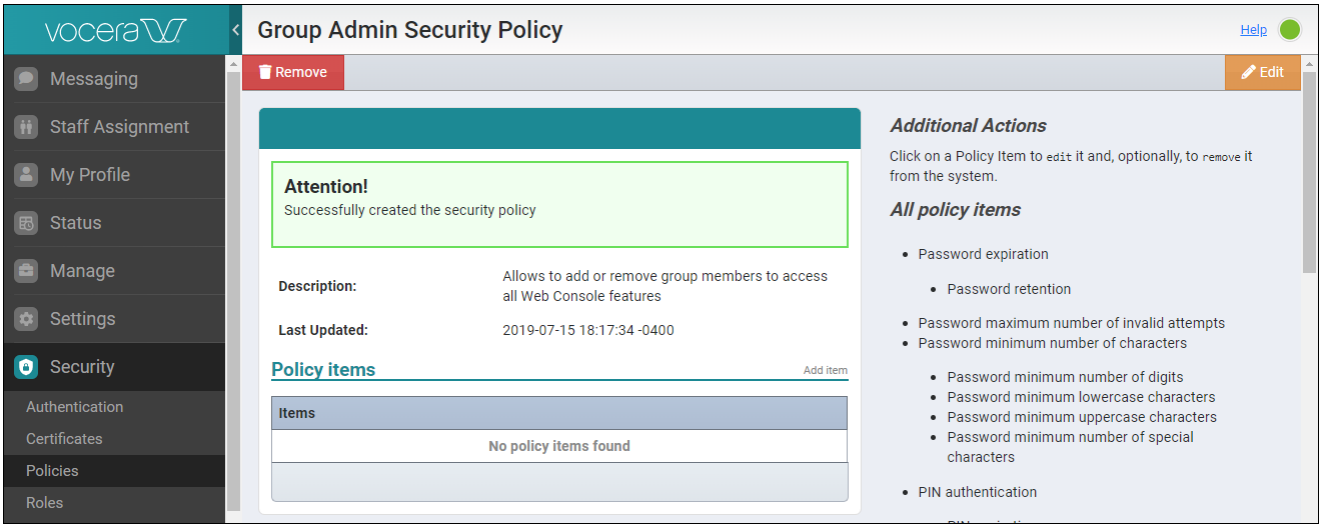


2. Complete the configuration fields for the new security policy.

Configuration Field	Description
Name	Enter a unique name to identify the new security policy in the system. For example, if you are creating a policy for Group Admin to add or remove group members who can access all Web Console features. You can enter a name, such as,"Group Admin." The Security Policy suffix is automatically added to the name of a policy.
Description	Enter a descriptive definition of the purpose of the new security policy.

3. Select one of the following to close the Create a New Security Policy dialog:
   - **Create** — to save the new security policy to the system.
   - **Cancel** — to return to the security policy list without saving the new security policy.

   If you selected **Create**, the new security policy is created and a success message displays. For example, the following screenshot shows a success message displayed after a policy named "Group Admin Security Policy" is created.



You can edit or delete this policy from the Web Console if needed.

What to do next:

After you create a new security policy, you can:

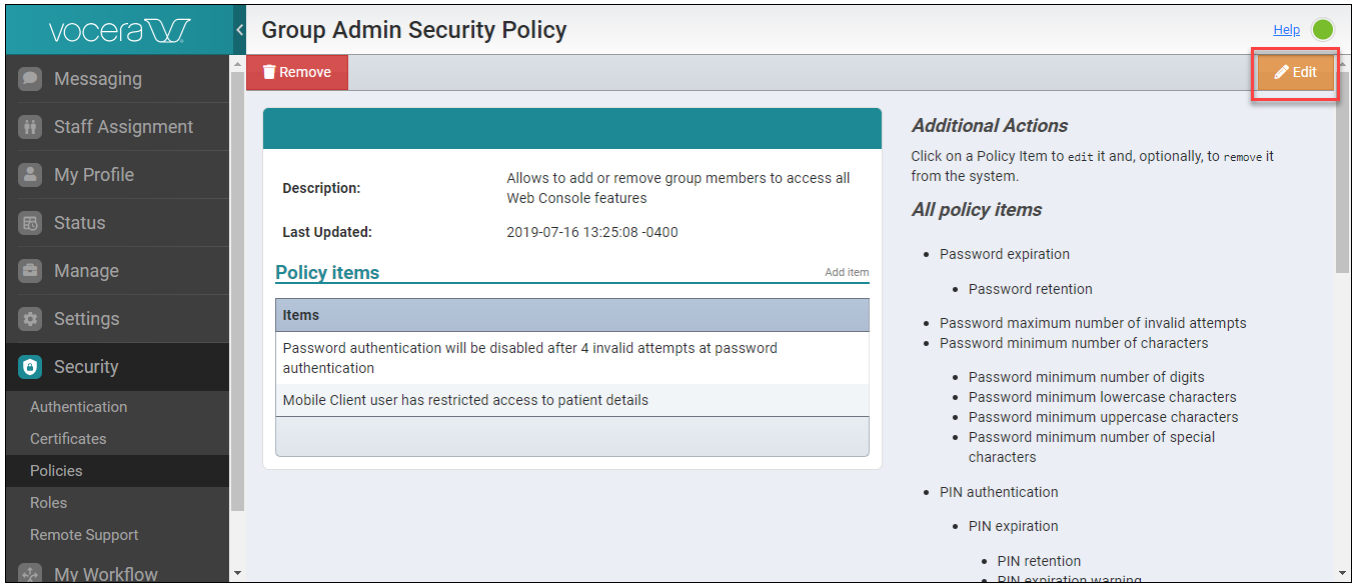
- Edit the name and description of this policy
- Add policy items to this policy
- Remove this policy from the system

Editing a Security Policy

A system administrator can revise an existing security policy and change the name and description of a security policy.

You cannot change the name and description for the Default security policy, but you can add or remove policy items from the Default security policy.

1. Click **Policies** in the **Security** section.
   The Security Policies page displays with a list of existing security policies in alphabetical order.
2. Select the security policy that you wish to revise and click the **Edit** button on the top right hand corner.
   For example, select an existing policy to edit, such as the policy named “Group Admin Security Policy” shown here, and click the **Edit** button.



The Update Security Policy page displays with fields that you can revise.

3. Revise the **Name** or **Description** fields in the Update Security Policy page.

Configuration Field	Description
Name	Enter a name that uniquely identifies the new security policy in the system.
Description	Enter a description defining the purpose of the new security policy.

4. Select one of the following to close the Update Security Policy page:
   - **Update** — to save the changes to the policy in the system.
   - **Cancel** — to return to the Security Policies page without making any changes.

Removing a Security Policy

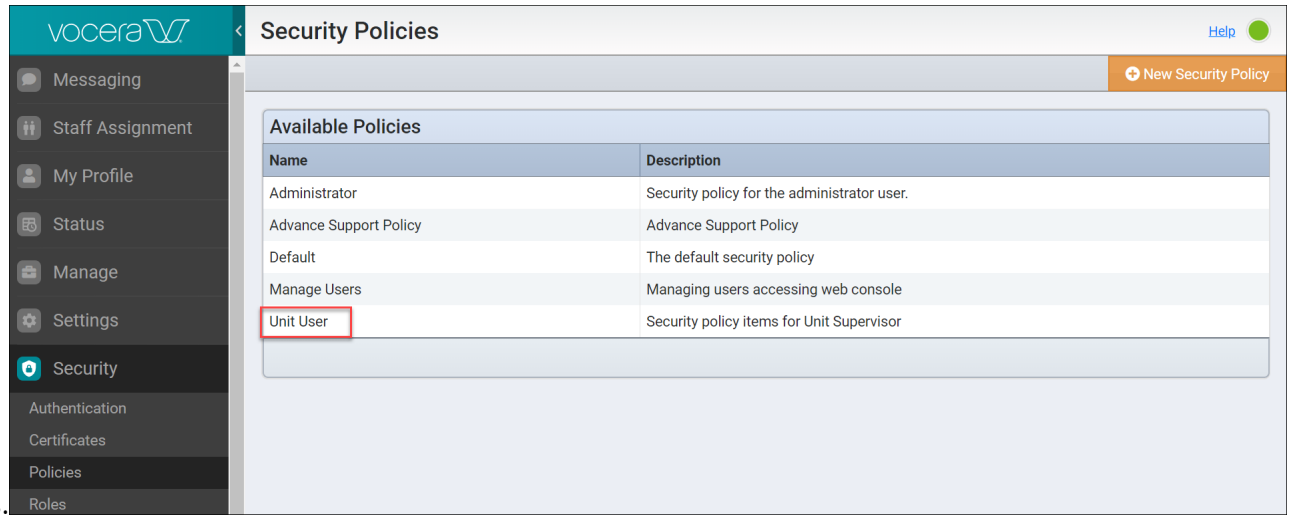
System administrators can remove an existing security policy from the Vocera system.

Before you remove a policy, review the following limitations:

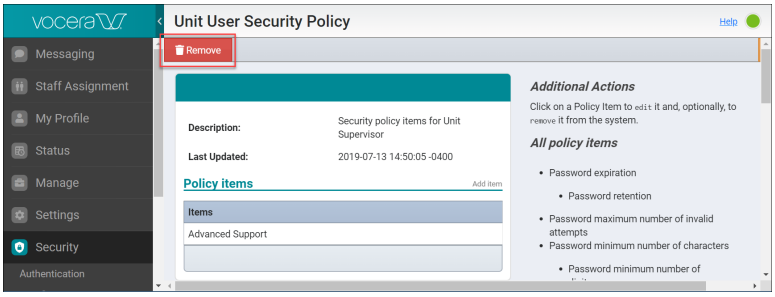
- You cannot remove the Default Security Policy.
- You cannot remove a policy if it is assigned to an existing role in the system.

1. Navigate to **Policies** in the **Security** section of the navigation bar.
   The Security Policies page displays with a list of available policies in the system.
2. Click on the policy that you want to remove from the system.

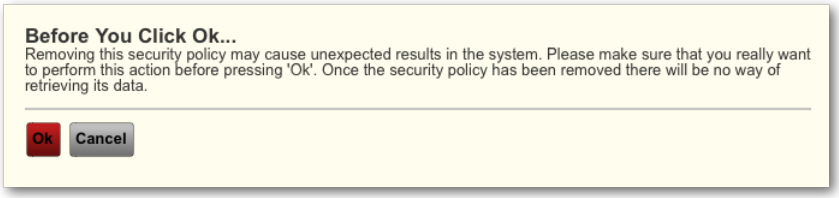
For example, if you clicked on an existing policy named “Unit User,” the Unit User page displays.



3. Click **Remove** in the selected policy page to remove the policy from the system.



A warning dialog displays to alert you about the unexpected results that may occur as a result of removing this policy from the system.



4. Select one of the following to close the warning dialog:
   - **Ok** — to confirm and remove the policy from the system.
     If you selected **Ok**, the policy is removed, and success message displays to confirm the removal.
   - **Cancel** — to cancel the delete action and return to the Security Policy page.

Understanding Security Policy Items

Policy items, such as session timeout or profile photo, are defined to manage user access to a particular function in Vocera when the item is applied via a security policy.

The Vocera policy items are described in detail here.

Console Session Timeout Policy Item

The "Console Session Timeout" policy item allows the users to remain inactive for a configurable amount of time before they are automatically logged out of the system.

When this policy item is added to a security policy, it allows the facility to establish how many minutes a user can remain inactive and logged into the system. Console Session Timeout (in minutes) must be between 1 and 10,000 minutes. The default value is 5 minutes, after which the browser requires a user to login again.

Console Session Timeout is one of the Policy Items in the Default Security Policy.

You can edit the configuration value or remove this policy item from the Default policy. See Editing a Policy Item on page 414 and Removing a Policy Item on page 415 for more information.

Console Access Management Policy Items

This section describes all policy items required to manage controlled access to the Vocera Platform Web Console.

Users with system administrator roles require an Administrative Security Policy to manage the user access to Web Console. The Administrator Security Policy may include the policy items listed in the following table.

Console group management allowed	Allows users to manage groups from within a single facility. When this policy item is applied to a security policy, group members assigned to a role associated with this security policy can view all groups in a specific facility, create and share templates with group members.
Console group member updates allowed	Allows a group of users to manage group membership from within a single facility When this policy item is added to a service policy, the Web Console displays only the groups that are within the facility with granted access.
Console reset password allowed	Allows a group of users to reset password for Web Console users. When this policy item is added to a service policy, group members assigned to a role with this policy item can reset passwords for the Web Console users.
Console system management allowed	Allows a group of users to manage group membership for a specific facility. When this policy item is added to a service policy, group members assigned to a role with this policy item can add or remove members to a group and perform group management activities, and create templates.
Console template management allowed	Allows a group of users to manage templates owned by a specific facility When this policy item is added to a service policy, group members assigned to a role with this policy item can manage the templates for groups within a facility.
Console user management allowed	Allows a group of users to manage users and contacts for a specific facility. When this policy item is added to a service policy, group members assigned to a role with this policy item can manage the users and contacts for groups within a facility.
Console user profile access allowed	Allows the system administrator to enable or disable user access to My Profile The My Profile section will not display in the navigation bar for a Group that doesn't have this policy item applied to it through a role.
Console Vocera device management allowed	Allows a group of users to manage and view the status of devices in a specific facility. When this policy item is applied to a Security Policy, group members assigned to a Role associated with this security policy can view devices for a specific facility in the **Status Monitor** section of the Web Console.

Maximum File Size of a User's Profile Photo Policy Item

The “Maximum file size of a user's profile photo” policy item limits the maximum file size allowed for a photo that is uploaded to a user account to display as an avatar in the Mobile client.

Vocera recommends a compressed passport style photo, with a maximum file size of 100 kilobytes. By default, the photo size is limited only by the size of the underlying database.

The file size value must be in the range of one to 2000 kilobytes.

You can create a security policy item to specify a file size allowed for photos. See Editing a Policy Item on page 414 for changing the default value. When one or more maximum photo file size security policy items are available for the facility, the policy item with the smallest file size value will be used as the maximum file size.

Mobile Client Security Policy Items

This section describes the available Mobile Client security policy items to enable access control over the user's mobile devices.

System administrators can design and customize the access and authentication features for mobile client users based on the mobile client security policies listed in the following table.

Note: In addition to the mobile client policy items, Vocera offers security policy items designed for Vocera Vina users. To learn more about these policy items, see the Vocera Vina Policy Items on page 411 section.

Policy Items	Description
Mobile Client device passcode required	Requires the user to set a device passcode in order to login .This passcode is a user's iOS or Android system passcode, biometrics or swipe code. Enforcing this policy ensures that users who bring their own devices have protected their device.
Mobile Client trusted certificate required	Prevents the user from accepting an untrusted certificate when logging in.
Mobile Client controls access to patient details	Controls access to patient details on the mobile client. This policy item includes two values: • restricted — the “restricted” access excludes patient records in roster search results and omits patient details displaying in a patient linked conversation • full — the “full” access permits patient records in the roster search results and includes all patient details in patient linked conversations. The “full” value is also the default value for this policy item. Vina does not implement "omits patient details showing in a patient linked conversation" at this time but Engage Mobile does.
Mobile Client inactivity timeout	Sets the amount of time (in minutes) the mobile client user can remain inactive in the application. When this time has elapsed with the app in the background, the user must re-authenticate before interacting with the app again. If PIN authentication is enabled, the user can enter either the PIN or the password to re-authenticate. If PIN authentication is not enabled, the user can enter their password for re-authenticate. The default value is 5760 minutes.

Password Authentication Policy Items

This section describes the available Password Authentication policy items that restrict users access to the Vocera system.

Password security policies only apply to user accounts created in the Vocera system.

System administrators can design and customize the access and authentication features for users based on the password authentication security policies listed in the following table.

Policy Items	Description
Password expiration	Adds a password expiration policy item to force passwords to expire after the configured number of days. Enabling Password Expiration means a value must be provided for the number of days before a password expires. Password Expiration (in days) must be between one and 1000. The default Password Expiration limit is 30 days.
Password retention	Restricts users from reusing one or more expired passwords. Users are unable to reuse a password as long as it is retained. Password retention (in days) must be between one and 1000. The default Password retention limit is 90 days. **Note:** You must enable the "Password expiration" policy item first in order to configure the "Password retention" policy item. Once the "Password expiration" policy item is enabled, the "Password retention" policy item is available to select from the drop down list.
Password maximum number of invalid attempts	Sets a limit for the maximum number of times users can attempt to enter their password. When the invalid attempts number is exceeded without entering the expected password, the user is locked out of the device. The default number of invalid attempts is 3. You can enter a value between 1 to 10 to set a limit to the number of invalid attempts.
Password minimum number of characters	Sets a limit to the minimum length for passwords regardless of the types of characters in the passwords. Password minimum number of characters must be between two and 64. The default value is 4 characters. The password minimum number of characters policy item is one of the policy items included in the Default Security Policy, and you can edit or remove this item from the Default policy.
Password minimum number of digits	Sets a limit to the minimum number of digits required in a password. You can add the Password Minimum Number of Digits policy item to a security policy if the Password Minimum Number of Characters is first configured in the policy. Adding this item requires passwords to contain a minimum number of numerical characters. Password Minimum Number of Digits must be between one and 64.
Password minimum number of lowercase characters	Sets a limit to the minimum number of lowercase (a-z) characters required for a password. Adding this item requires passwords to contain a minimum number of lowercase characters. You can configure a value between 1 to 64. The default value for Password minimum number of uppercase characters is one. You must configure the "Setting Password Minimum Number of Characters" policy item before configuring this policy item.
Password minimum number of uppercase characters	Sets a minimum number of uppercase character requirement for a password. Adding this item requires passwords to contain a minimum number of uppercase (A-Z) characters. You can configure a value between 1 to 64. The default value for Password minimum number of uppercase characters is one. You must configure the "Setting Password Minimum Number of Characters" policy item before configuring this policy item.
Password minimum number of special characters	Sets a minimum number of special character requirement for a password. Adding this item requires passwords to contain a minimum number of special characters. You can configure a value between 1 to 64. The default value for Password minimum number of special characters is one. You must configure the "Setting Password Minimum Number of Characters" policy item before configuring this policy item.

Policy Items	Description
	For a list of supported special characters, see the Supported Special Characters on page 409 section.

Supported Special Characters

The following table displays a list of supported special characters include:

Symbol	Name	Symbol	Name	Symbol	Name	Symbol	Name
	Space	,	Comma	.	Period	?	Question Mark
;	**Semicolon**	:	Colon	-	Hyphen	'	Apostrophe
"	**Quotation Mark**	!	Exclamation Mark	@	At Sign	#	Number Sign
$	Dollar Sign	%	Percent Sign	^	Caret	&	Ampersand
*	Asterisk	(	Open Parenthesis	)	Close Parenthesis	+	Plus Sign
/	Slash	<	Less Than	=	Equal Sign	>	Greater Than
[	Open Bracket	\	Backslash	]	Close Bracket	_	Underscore
'	Accent	{	Open Brace	|	Vertical Bar	}	Close Brace
~	Tilde						

PIN Authentication Policy Items

This section describes the available PIN Authentication policy items that enforce a secondary layer of user authentication on Vocera devices.

PIN authentication acts as a secondary layer of authentication, and it allows control over user access to the Vocera system from supported devices and mobile clients.

You must enable the PIN Authentication policy item to add additional PIN policy items, as described in the following table:

PIN Authentication Policy Items	Description
PIN authentication	Enables PIN authentication for users.
PIN expiration	Configures PIN expiration (in days) to allow PINs to expire after the configured number of days. Enabling PIN expiration requires a value to be provided for the number of days before expiration. You must enable PIN authentication to configure PIN expiration. The default value is 30 days. To learn how to change the default value, see Editing a Policy Item on page 414.
PIN retention	Restricts users from reusing one or more expired PINs; setting PIN retention prevents users from reusing a PIN as long as it is retained. You must enable PIN expiration to configure PIN Retention. The default value is 90 days. To learn how to change the default value, see Editing a Policy Item on page 414.
PIN expiration warning	Plays a warning message on a Vocera device enabled for PIN authentication. You can enter a value within the range of one to 1000 days. The default value for PIN expiration warning is 3 days.
PIN minimum number of characters	Sets a minimum character limit for PIN length. The default character limit is 4 characters. See Editing a Policy Item on page 414 to learn how to change the default value. You must enable PIN authentication to configure this policy item.
PIN maximum number of invalid authentications	Sets a maximum limit for unsuccessful PIN login attempts. When the maximum number of login attempts is exceeded, the user's PIN must be updated in the user's account. You must enable PIN authentication to configure this policy item. You can enter a value within the range of one to 10. The default value is 3 invalid attempts. To learn how to change the default value, see Editing a Policy Item on page 414.
PIN authentication bypass for Cisco phones	Enables PIN authentication bypass for Cisco phones for a policy while the Cisco Unified Communications Manager adapter has a default user with this policy assigned so that users are not required to login to Vocera Platform from Cisco phones. This policy applies only to Cisco phones. For detailed configuration information, refer to the Vocera CUCM Adapter documentation available on the Vocera Documentation Portal.
PIN authentication bypass for SpectraLink XML phones	Enables PIN Authentication Bypass for SpectraLink XML phones for a policy while the SpectraLink XML adapter has a default user with this policy assigned so that users are not required to login to Vocera Platform from SpectraLink phones. This policy applies only to SpectraLink XML phones. For detailed configuration information, refer to the Vocera SpectraLink XML Adapter documentation available on the Vocera Documentation Portal.

Staff Assignment All Department Access Policy Item

The “Staff Assignment all department access” policy item controls user access to all departments in the Staff Assignment application.

The Staff Assignment system administrator can add the “Staff Assignment all department access” policy item to a Staff Assignment security policy and assign this policy to the Administrator role or Default role. Adding this policy item allows the users to view and update assignments for all departments in the Staff Assignment application.

There are no configurable values for this policy item. You can remove this item to disable access to all departments in the Staff Assignment application.

You can add or remove this policy item from the Default policy. See Adding a Policy Item and Removing a Policy Item on page 415 for more information.

Vocera Vina Policy Items

This section describes the available Vocera Vina specific policy items available to enforce access control and secure authentication for Vocera Vina users.

Important: In addition to the Vocera Vina security policy items described in the following table, Vocera offers security policy items designed for mobile client users. To learn more about these policy items, see the Mobile Client Security Policy Items on page 406 section.

Policy Items	Description
PIN Authentication	Enables PIN authentication for Vocera Vina users. The Vocera Vina users can use their Vocera PIN to re-authenticate when an inactivity timeout occurs. Users must set a PIN at login, if they haven't set a PIN, the existing PIN is expired, or it is locked. For additional PIN policy items, see the policy items described in the PIN Authentication Policy Items on page 409 section.
Vocera Vina controls the ability for clients to customize tabs	Allows clients to customize tab names.
Vocera Vina uses the default name for custom tab 1	Configures a default name for custom tab 1. A system administrator can enable this policy item to control the default name for a custom tab. For more information on configuring default name for custom tabs, see Configuring Default Name for Custom Tabs on page 411
Vocera Vina uses the default name for custom tab 2	Configures a default name of custom tab 2. A system administrator can enable this policy item to control the default name for a custom tab. For more information on configuring default name for custom tabs, see Configuring Default Name for Custom Tabs on page 411
Vocera Vina is enabled for debug logging	Enables debug logging for Vocera Vina clients. Debug logging is disabled when this policy item is removed from the policy.
Vocera Vina allows using biometric unlock	Enables biometric authentication for Vocera Vina clients. When this policy item is added, users can use the TouchID or Fingerprint ID on their Android or iOS mobile clients to access the Vocera Vina app instead of using an app PIN. This policy item is useful for Vocera Vina users who bring their own devices (BYOD). A system administrator can look up the device inventory and confirm if the devices **Is Shared** or personal If the device is not shared, users for this personal device can use the biometric authentication.
Vocera Vina Disconnect Timeout	Sets a maximum amount of time (in minutes) for which the Vocera Vina application may be disconnected from the server before being automatically logged out. The Vocera Vina application uses this time to refresh the security access with the Vocera Platform server. You can enter a value within the range of one to 10080 The default value is 5760 minutes.

Configuring Default Name for Custom Tabs

Configure a default name for custom tabs using the custom tab policy items.

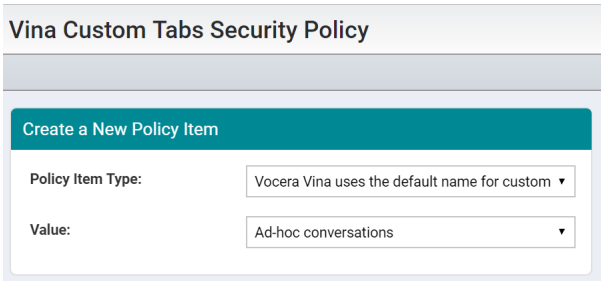
A system administrator can configure a default name for custom tabs in the Vocera Vina app to control the default name for the custom tabs.

1. Create a new security policy for the custom tabs, see Creating a Security Policy on page 401
   You can also edit an existing policy and add the custom tab policy items to this policy.

2. Click **Add items** and select the "Vocera Vina uses the default name for custom tab 2" security policy item.
   a. Select a value for the "Vocera Vina uses the default name for custom tab 2" security policy item from the drop down list.

      You can select one of the following values:
      - Ad-hoc conversations
      - Archive
      - My Patients
      - Patients Linked conversations

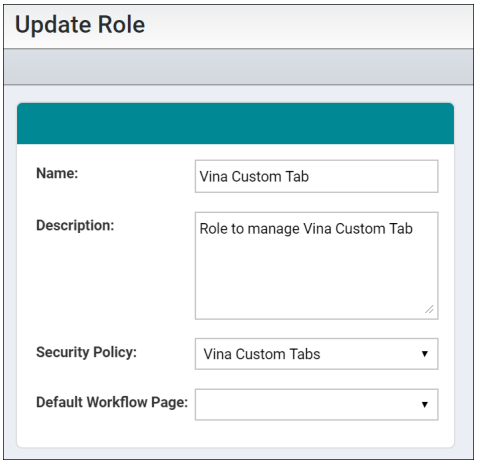
      For example, in the following screenshot, Adhoc Conversations is selected as the value for the "Vocera Vina uses the default name for custom tab 2" policy item. This value will appear as a default tab name on the Vocera Vina app.



   b. Click **Add** to add this policy item.
3. Select a value for the "Vocera Vina uses the default name for custom tab 1" security policy item from the drop down list.
   a. Select a value for the "Vocera Vina uses the default name for custom tab 1" security policy item from the drop down list.
   b. Click **Add** to add this policy item.
4. Navigate to **Roles** in the **Security** section and select a Role to assign the custom tab security policy.

   If you don't have an existing role for custom tab, you can create a new role. See Adding a Role on page 418 for information on creating a new role.
5. Select the custom tabs security policy that you created in Step 1 from the Security Policy dropdown list.

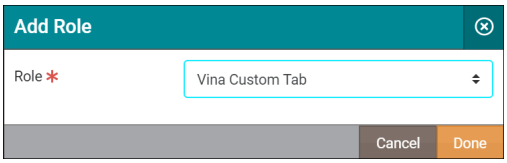
   For example, the following screenshot shows the Vina Custom Tabs security policy selected for the Vina Custom Role.



6. Click **Update** to save the changes.
7. Navigate to **Groups** in **Manage** section and locate the group responsible for custom tab management.

If you don't have an existing group responsible for custom tab management, you can create a group, see Adding a Group on page 170 for information on creating a new group.

8. Select the custom tab management group to open the Edit Group page, and scroll down to the **Roles** section.
9. Click **Add Role** to associate the Vina Custom Role with this group, and click **Done** to associate the selected role.



10. Click **Save** to save changes to the custom tab management group.

Managing Security Policy Items

Security policy items are enabled within a specific security policy to establish a limited set of permissions.

Each security policy can have one or more policy items that apply to any Roles on page 417 associated with the security policy.

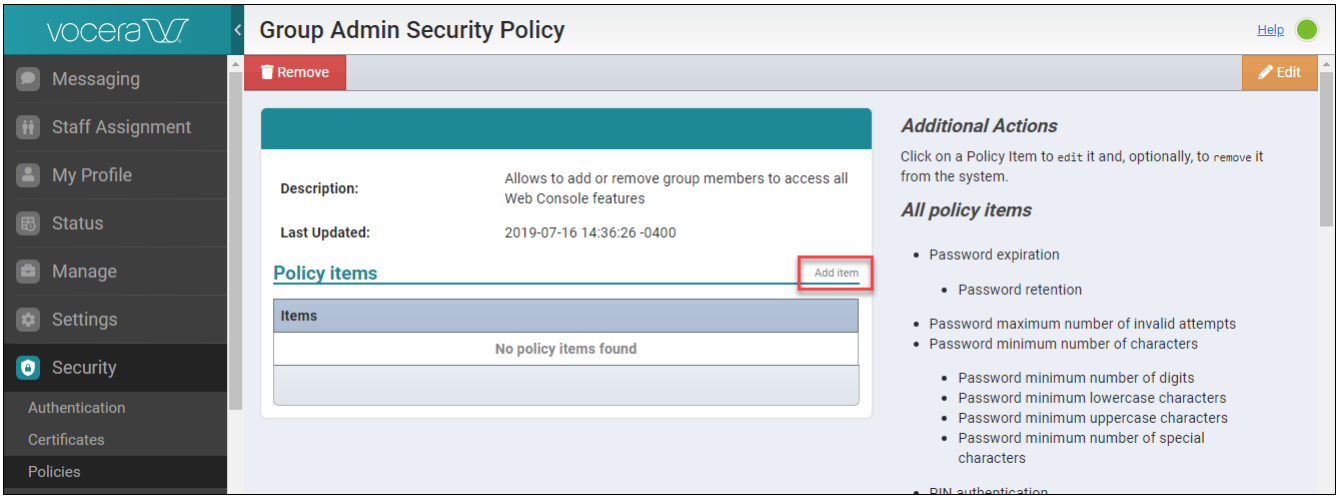
This section describes how you can add, edit, or remove policy items in the Vocera Platform Web Console

Adding a Policy Item

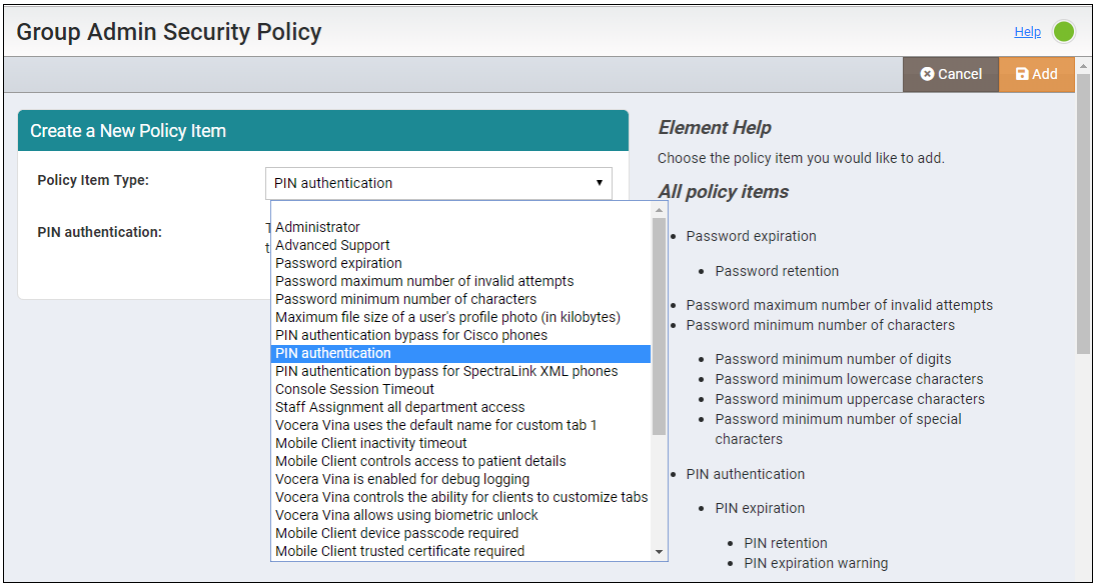
A system administrator can add policy items to a security policy and customize the security policy.

Before you begin:
Review the available policy items and configurable values for the policy items described in the Understanding Security Policy Items on page 404.

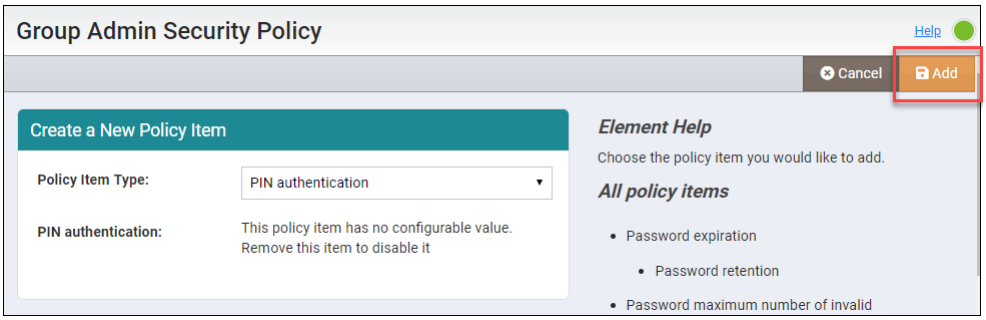
1. Navigate to **Policies** in the **Security** section, and click on a security policy from the list.
   The selected security policy page displays.
2. Click **Add item** to add policy items to the security policy.



3. Click the arrow head next to the **Policy Item Type** field to display the available policy item types.



4. Select one of the following to close the security policy page:
   - **Add** — to add the selected policy item to the security policy.
     For example, the following screenshot shows the PIN authentication policy item selected for the "Group Admin Security Policy ."



     If you selected **Add**, the policy item is added to the security policy and system displays a success message to confirm the addition of the policy item.
   - **Cancel** — to return to the security policy page without adding the policy item.

What to do next:

After you add a policy item, you can:
- Repeat this task to add more policy items.
- Edit the configurable values for a policy item.
- Remove a policy item.

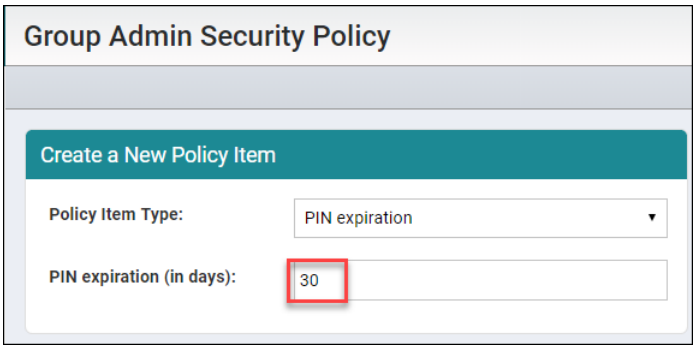
Editing a Policy Item

A system administrator can edit configurable values for an existing policy item.

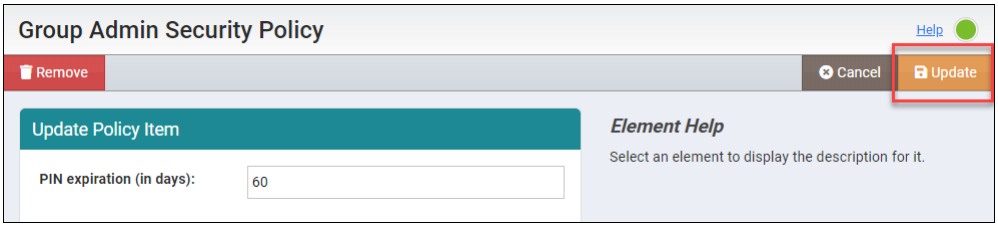
Note: Not all policy items have a configurable value that you can edit. You can only add or remove the policy items that do not have a configurable value.

For example, you can only add or remove a PIN authentication policy item. However, if your security policy contains a PIN expiration policy item, you can replace the default PIN expiration value (30 days) with a value with a new value.

1. Navigate to **Policies** in the **Security** section, and click on a security policy that contains the policy item that you want to edit.
   The selected security policy page displays.
2. Click on the policy item that you want to edit.
   For example, if you have a "PIN expiration" policy item, you can to change the default expiration value of 30 days to 60 days.



3. Replace the existing or default value with a value of your choice.
4. Select one of the following to exit the security policy page:
   - **Update** — to update the selected policy item.
     For example, the following screenshot shows the default value for PIN expiration policy item changed to 60 days. When you click **Update**, the system displays a message to confirm that the policy item was successfully updated.

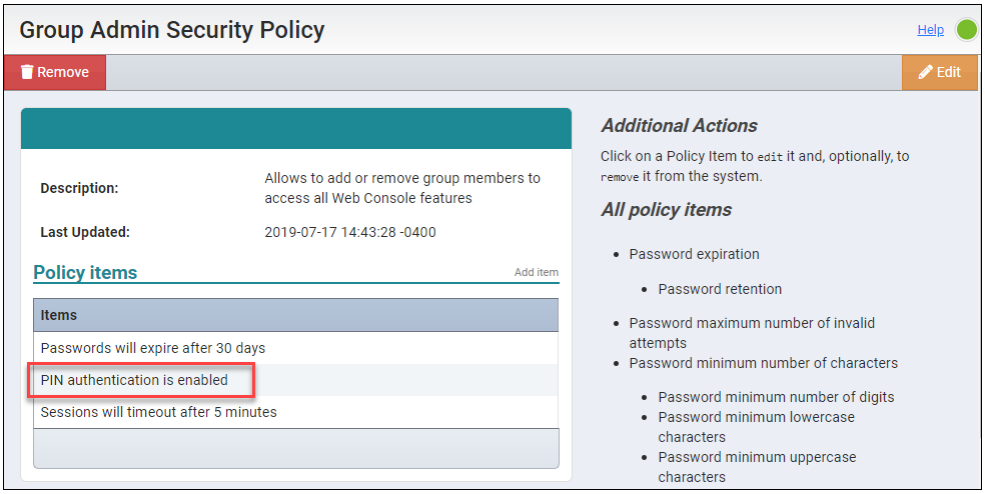


   - **Cancel** — to return to the security policy page without updating the policy item.
   - **Remove** — to remove the policy item.

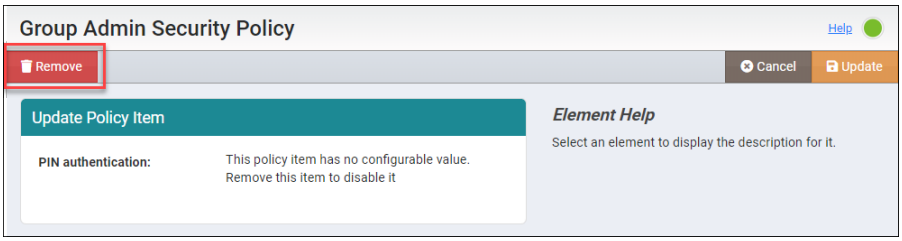
Removing a Policy Item

A system administrator can delete a policy item from an existing security policy.

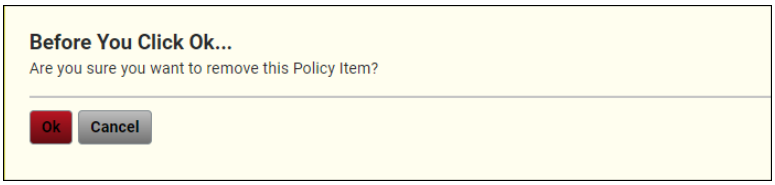
1. Navigate to **Policies** in the **Security** section, and click on a security policy that contains the policy item that you want to remove.
   The selected Security Policy page displays.
2. Click on the policy item that you want to remove from the Policy Items section.
   The security policy page displays the Policy Items section with a list of available polity items. You can select a policy item that you want to remove from the list.
   For example, if you want to delete the **PIN authentication is enabled** policy item, you can click and select this item.



3. Click **Remove** to remove the selected policy item.



The system displays a warning dialog to confirm if you want to remove the selected policy item.



4. Select one of the following to close the warning dialog:
   - **Ok** — to confirm and remove the policy item from the system.
     If you selected **Ok**, the policy item is removed. A success message displays to confirm the removal of this policy item from your system.
   - **Cancel** — to cancel the remove action and return to the Security Policy page.

Roles

Roles determine user access to information presented in the Vocera system.

In Vocera Platform, Roles function as the gatekeepers to the information that is stored within and presented in the Web Console.

Users may or may not have permissions to access certain Vocera features in Web Console depending on the roles associated with the group to which they belong.

Vocera roles have one or more policies (aka security policies) defined and applied to them. Security policies grant or deny permissions to access the Vocera features. Users who are members of a specific group are associated with predefined roles as needed to access and manage the Vocera system.

Important: The Vocera Platform user account behavior is dependent on the policies assigned to a role.

To understand how users are associated with groups, roles, and policies see Understanding Groups, Roles, and Policies on page 168. Group members assigned to a predefined role have access to information in the system based on the security policies associated with each role. If a user is the member of a group, associating a role with this group will apply the security policy to a user's profile immediately.

In addition to policies, roles may also have a default workflow page associated with them. You can create new roles and apply customized workflow pages for a particular role requirement in your organization. See the Creating a New Workflow on page 312 for information on workflows.

Vocera system creates the following predefined roles at the time of installation:

- Administrator
- Default

You can access these roles in the Vocera Platform Web Console and associate these roles with groups in your system. See Accessing Roles on page 418 and Associating Roles with Groups on page 420 for more information.

An administrator role grants users access to the Web Console features. Group members with administrator role manage Vocera features, such as granting the user the ability to view audit logs, manage other users, and manage connected devices.

The Default role is assigned to all users who login to access the Web Console.

LDAP Group List

Some organizations use lightweight directory access protocol (LDAP) or ActiveDirectory server authentication that allows a user to login with the same credentials they use elsewhere in their office. The LDAP authenticated system may provide a predefined list of groups that you can utilize to assign a Vocera role and control information access.

For example, you can create a Clinician role in Vocera and associate it with the ActiveDirectory or LDAP Physicians group.

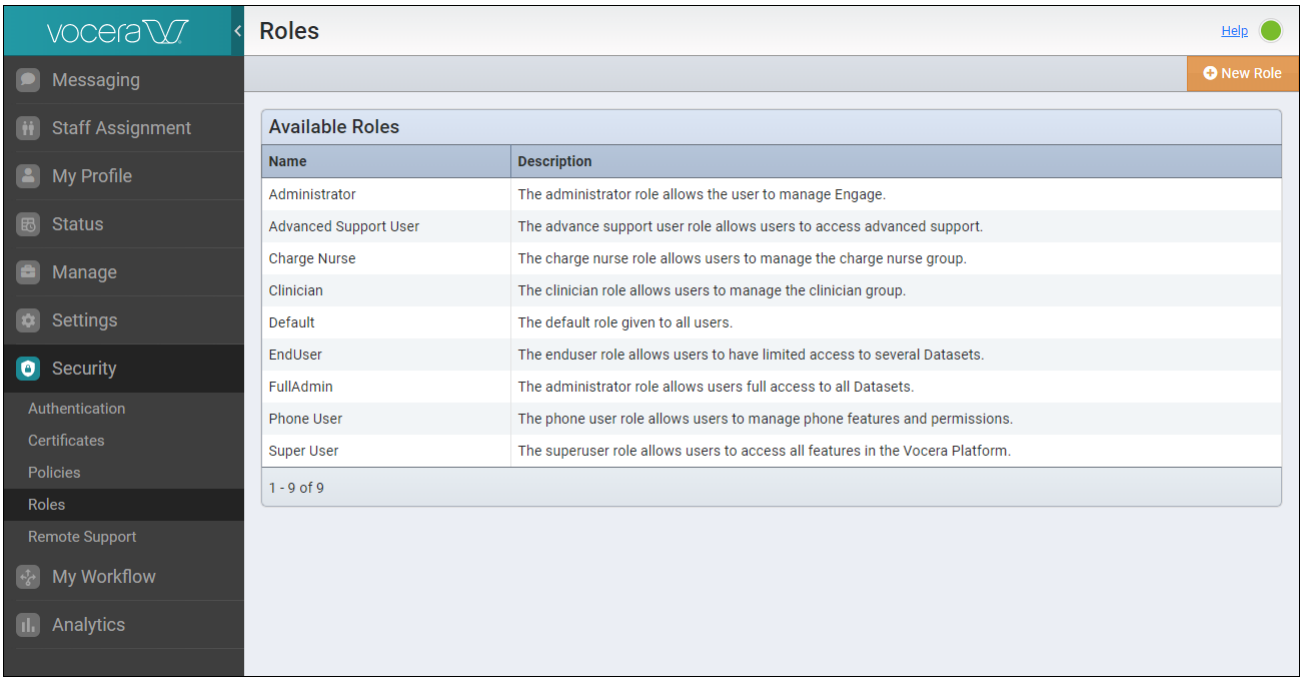
Accessing Roles

View and access the roles defined for your system.

Before you begin, understand how roles, users, groups, and policies are associated. See the Understanding Groups, Roles, and Policies on page 168.

The **Roles** page in the Vocera Platform Web Console allows you to add, edit, or delete a role.

1. Navigate to **Roles** in the **Security** section of the navigation bar.
   The Roles page displays a list of roles that are available on the Vocera system. The list is presented in alphabetical order, and displays a description for the role.
   The following screenshot is an example of some roles that you can create in your system. The Administrator role and the Default roles are created by the system at the time of installation.



2. Click on a role in the list to view or edit its detail.
   You can also select the **New Role** button to create an additional role, modify an existing role, or delete roles from the Web Console

Note: You cannot delete the Administrator and Default roles created at the time of Vocera system installation.

What to do next:

- See Adding a Role on page 418 to add new roles.
- See Editing a Role on page 420 to edit an existing role.

Adding a Role

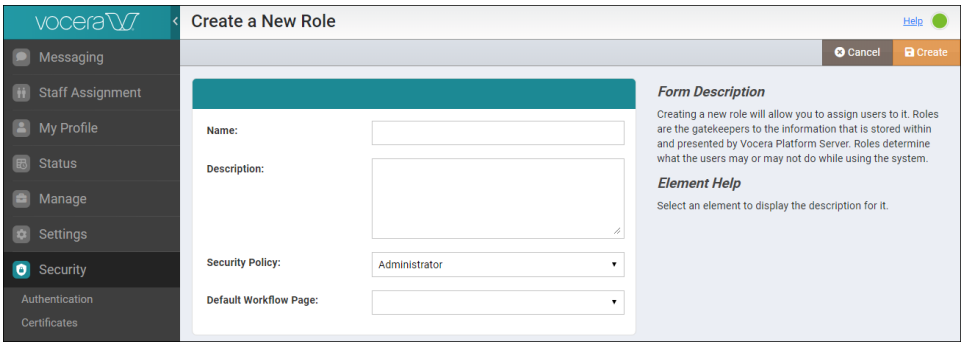
Define and add a new role to the list displayed in the Vocera Platform Web Console.

Before you add a new role, review the following:

- A role can have only one security policy associated with it.
- Each security policy can have one or more policy items.
- A group can have multiple roles associated with it and a role can have multiple groups associated with it.

The Administrator and Default roles are created at the time of Vocera system installation. You can add several new roles to the system as needed.

1. Navigate to **Roles** in the **Security** section, and click **New Role**.
   The **Create a New Role** page displays:

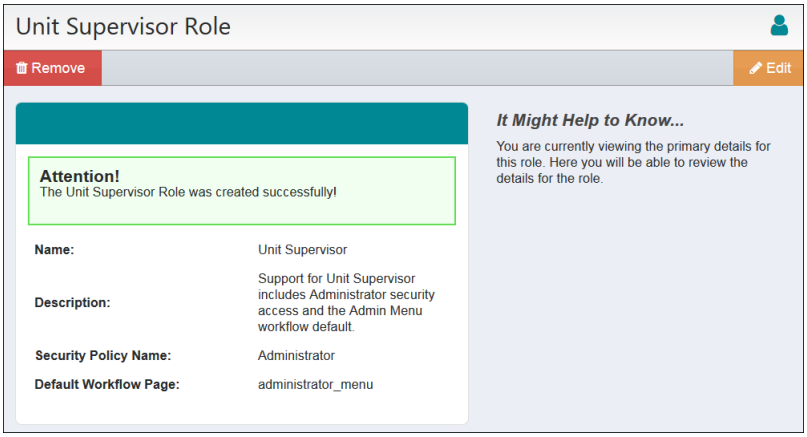


2. Complete the configuration fields listed in the following table:

Field	Description
Name	Enter a name to uniquely identify the new role.
Description	Describe the purpose of the new role. Include details of what actions the role will allow the user.
Security Policy	Select a security policy from the dropdown list. The selected policies are applied to all users assigned the new role.
Default Workflow Page	Select a workflow page from the dropdown list. The selected workflow page will be presented by default to each user assigned the new role. The workflow page is used as the entry point to Vocera on the user's device.

3. Select one of the following to close the Create a New Role dialog:
   - **Create** — to add the new role to the system.
   - **Cancel** — to return to the Roles page.

   If you selected **Create**, the new role is created and a success message displays. You can edit or delete this role from the Web Console, if needed.



What to do next:

After you create a role, you can associate this role with a group. See Associating Roles with Groups on page 420 for more information.

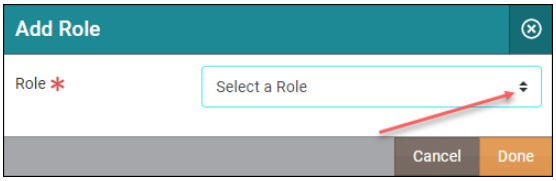
Associating Roles with Groups

Roles associated with a group or groups control the availability of Vocera Platform Web Console features for group members.

Before you begin:

- Be cautious when assigning roles to groups and users to groups associated with specific roles.
- Remember that group members inherit access privileges based on the roles assigned to their group.
- Create roles before associating them with an existing group or groups.

1. Navigate to **Groups** in the **Manage** section and locate the group the you want to associate a role with.
2. Click on the name of the group that you want to edit.
   The Edit Group page appears.
3. Scroll down to the Roles section and click **Add Role** to associate a role with this group.
   The Add Role dialog box appears.
4. In the Add Role dialog box, choose a role from the Select a Role dropdown list, and click **Done**. Repeat this step to add additional roles for this group.

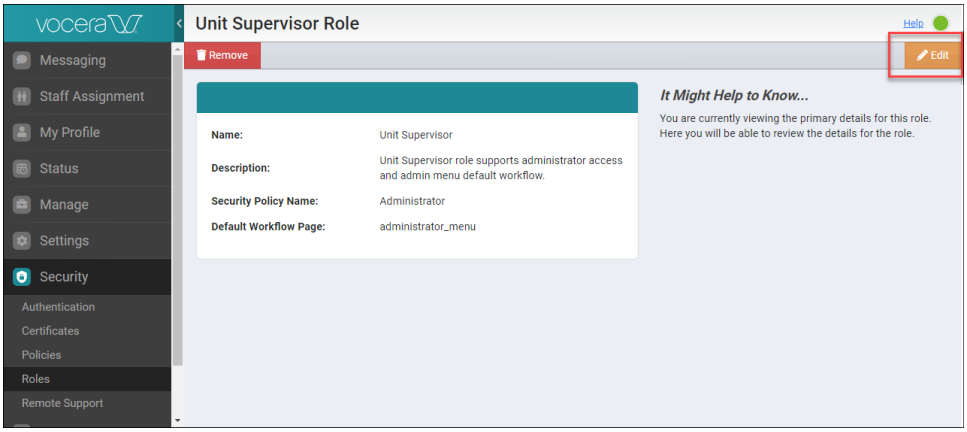


Editing a Role

System administrator can modify the name, description, security policy, and workflow for an existing role.

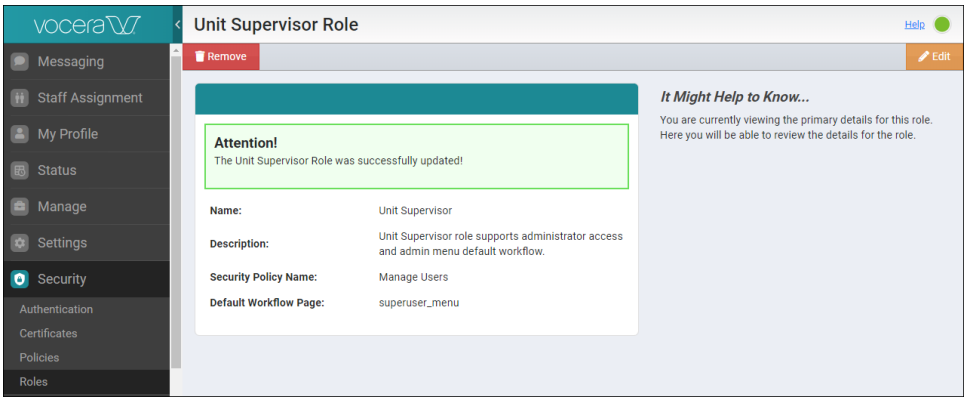
The only exception to editing existing roles in the system is the predefined Administrator role created at the time of Vocera Platform installation. You cannot change the name or description of the Administrator role created at the time of installation, but you can change the security policy and the workflow page associated with this role.

1. Click **Roles** in the **Security** section.
   The Roles page displays with a list of available roles in the system.
2. Click on the role that you want to edit.
   The selected Role's page displays with detailed information on this role. From a Role's page you can choose to edit or remove the role from the system.
   For example, if you want to edit an existing role named, “Unit Supervisor Role”, clicking on this role will launch the Unit Supervisor Role page. You can click the **Edit** button as shown in the following screenshot to redefine the configuration fields for this role.



3. Select the **Edit** button in the right hand corner to access the configuration fields to redefine the role. The **Update Role** page displays.
4. Edit the role information as necessary. See Adding a Role on page 418 for a description of the configuration fields.
5. Select one of the following to close the Update Role page:
   - **Update** — to save the changes to the role in the system.

     When you click **Update**, the role is updated for the changes, and a success message displays, as shown in the following screenshot.



   - **Cancel**— to return to the Roles page.

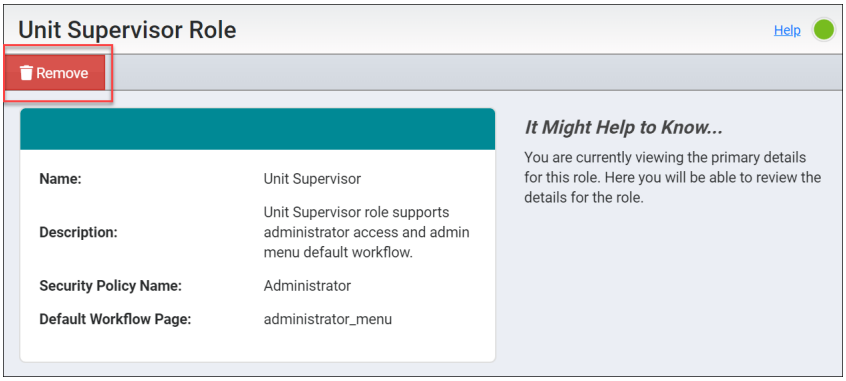
Removing a Role

Barring the Administrator role, you can remove any existing role in the system.

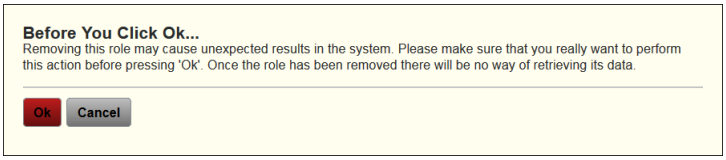
You cannot remove the Administrator role from the system, but you can revise the security policy and the workflow page associated with it if needed.

Attention: Removing a role may cause unexpected results in the system. Once a role is removed, you cannot retrieve the data associated with the role.

1. Navigate to **Roles** in the **Security** section of the navigation bar.
   The Roles page displays with a list of available roles in the system.
2. Click on the role that you want to remove from the system.
   For example, if you clicked on an existing role named, “Unit Supervisor Role”, the Unit Supervisor Role page displays.
3. Click **Remove** in the selected role page to permanently remove the role from the system.



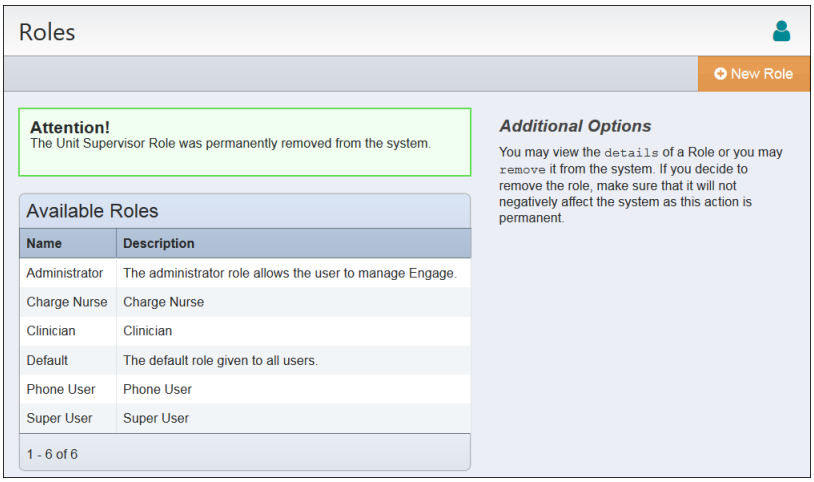
A warning dialog displays to alert you about the unexpected results that may occur as a result of removing this role from the system.



4. Select one of the following to close the warning dialog:
   - **Ok** — to confirm and remove the role from the system.

     Remember: Removing the role is an irreversible action, and you cannot retrieve the role's data after it is removed from the system.

     If you selected **Ok**, the role is permanently removed, and a success message displays to confirm the removal of this role from your system.



   - **Cancel** — to cancel the delete action and return to the **Roles** page.

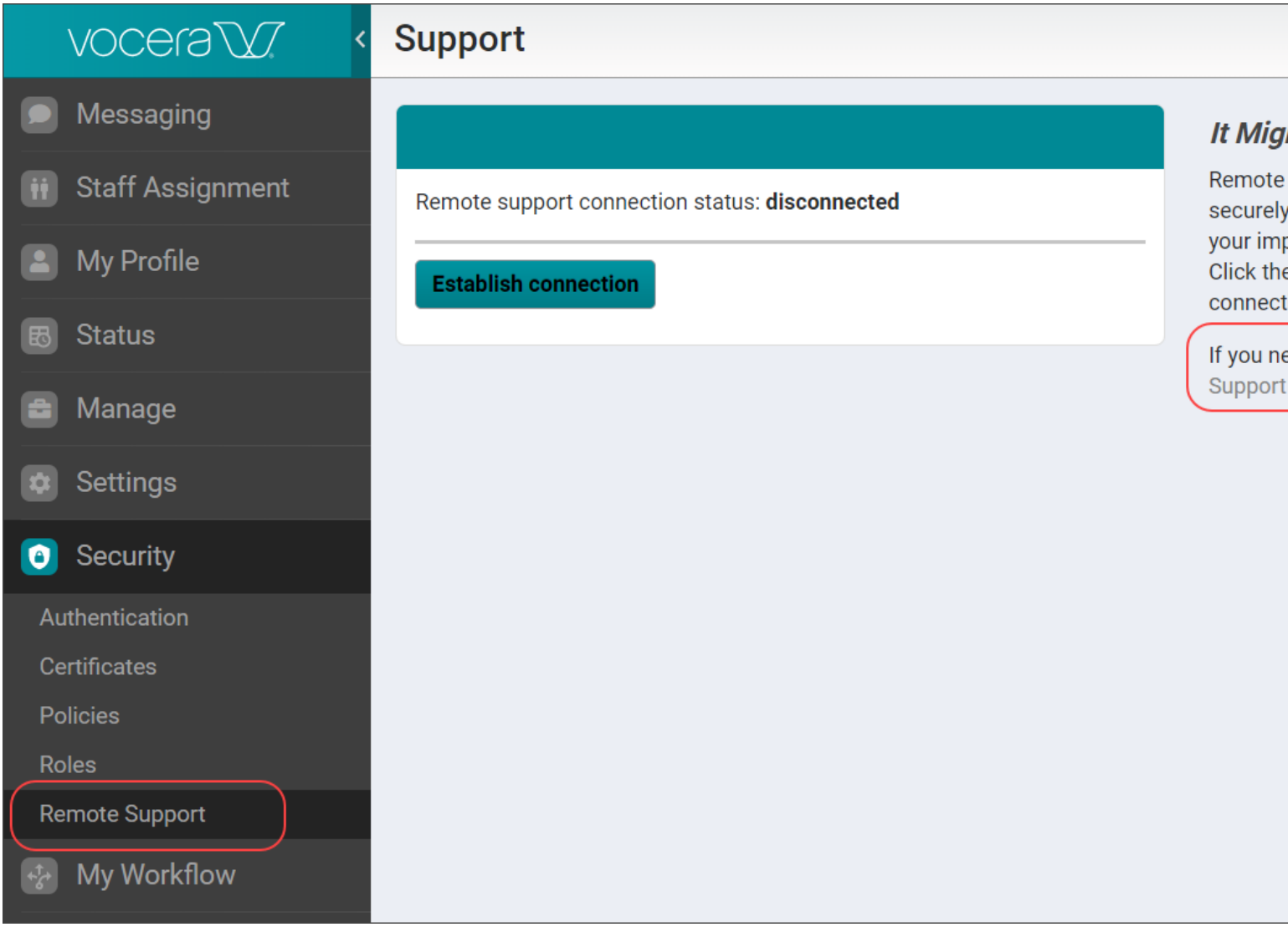
Remote Support

Remote support enables a secure connection between a Vocera system and an off-site Vocera support specialist.

To ensure the security of Vocera systems, a remote support session can only be initiated by an administrative user from the Vocera Platform Web Console. A System Administrator will initiate a remote support session in order to provide a Vocera support person access to the system.

Although Vocera has implemented multiple layers of protection to ensure the security of each installation during remote support, it remains good practice to only initiate remote support sessions when necessary and to end sessions as soon as they are finished.

Navigate to **Remote Support** in the Vocera Platform Web Console to establish and then disconnect a remote support session. If you need assistance, click the **Support** link in the "It might help to know..." section of the Vocera Platform Web Console to access the Vocera Support Services website.

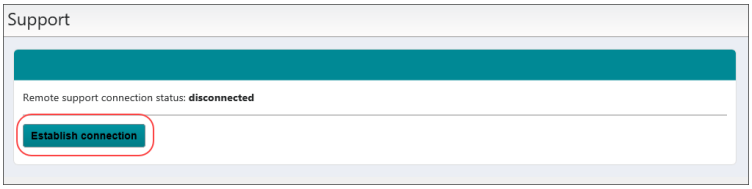


Establishing a Remote Session

Initiate a remote session to allow the support personnel access to the Vocera system.

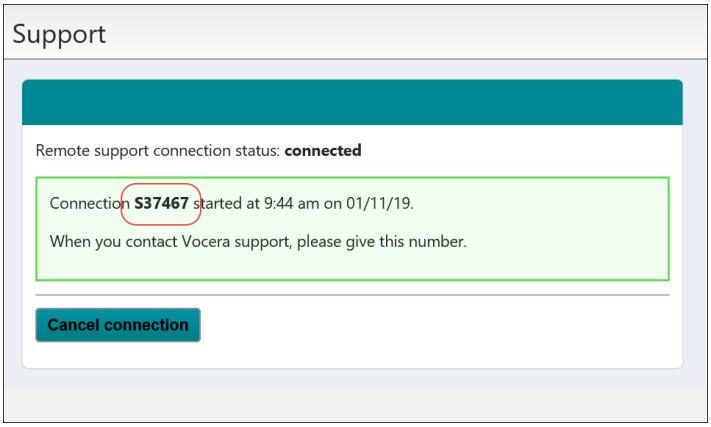
Note: Vocera Platform uses an outgoing TCP connection on Port 22 to `svc.ext-inc.com` for a remote support session.

1. Select **Remote Support** in the Security section in the Vocera Platform Web Console.
2. Select **Establish Connection** in the Support page.



3. Provide the connection ID to Support personnel.

   Once a session is initiated, the Support page displays an alphanumeric connection ID; S#####, where # represents the digits in the ID. When you contact Support, you must provide this ID to the support personnel in order to allow them access to your system.



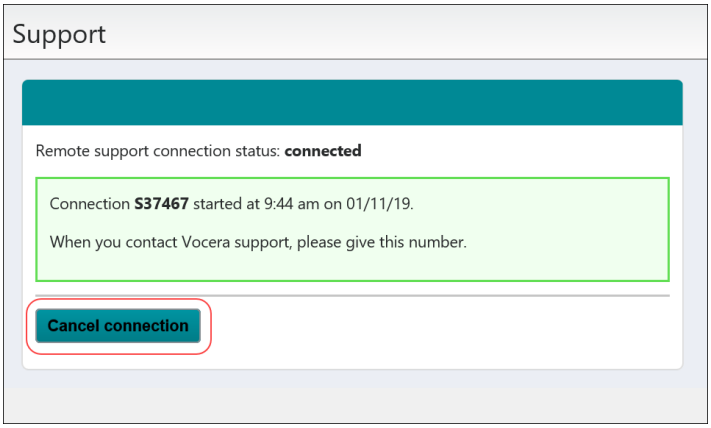
What to do next: See Disconnecting a Remote Session on page 425 for instruction on terminating the session.

Disconnecting a Remote Session

Disconnect a remote session after the support personnel completes the requested support work.

Note: Remember to end the remote support sessions as soon as the support tasks are completed.

1. Select **Remote Support** in the Security section in the Vocera Platform Web Console.
2. Select **Cancel connection** in the Support page.



A "Please wait..." message displays until the session is disconnected.

My Workflow

This section provides an overview of the Vocera Platform My Workflow Guide features.

- About the Vocera Platform My Workflow Guideon page 427
- The My Workflow Home Screen Layouton page 428

About the Vocera Platform My Workflow Guide

The Vocera Platform My Workflow Guide describes how to perform tasks using the My Workflow feature.

You can use this document as you work with My Workflow in the Vocera Platform Web Console. The organization of this guide generally matches the layout of the My Workflow console.

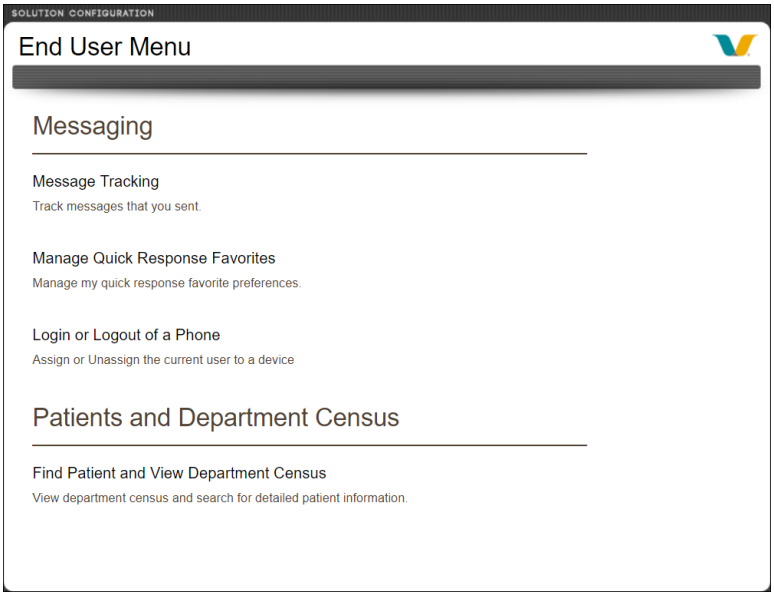
Selecting My Workflow displays the Menu screen, which allows users to access Vocera workflows via a web browser to perform specific tasks. For example, a Department Secretary can track alerts using My Workflow.

Note: Any hospital may include additional options to those described in this My Workflow documentation. Depending on the solution installed in your facility, you may see additional options that may not be described in this document.

The My Workflow Home Screen Layout

My Workflows displays a menu of the workflows available based on your roles and privileges.

Select **My Workflow** in the Vocera Platform Web Console to access the workflows, as shown in the following example.



By default, Vocera's My Workflows functionality provides access to a set of workflows for four pre-defined user roles; End User, Charge Nurse/Department Secretary, Super User, and Administrator. These default roles allow users to efficiently perform their responsibilities from the workflow menu displayed in a web browser.

Each menu is divided into two or more sections which may include the following:

- Messaging
- Configuration
- Monitor Tech
- Patients and Department Census

The user roles and the default workflow privileges allowed for each of the four roles described in this My Workflow documentation are provided as common example configurations. Hospitals may modify the name of the "Roles" or create additional roles to reflect the structure of the facility. For example, the End User role can view their assigned unit census, while the Administrator role can create a new unit in the facility.

Note: Workflows may not be enabled in your facility's implementation; contact a System Administrator for assistance.

Matrix of Workflows and User Roles

You can access workflows based on the roles associated with your profile in order to perform tasks in Vocera Platform Web Console.

Not all of the following workflows are available in the solution, and therefore may not be available in your facility. For example, the Staff Assignment workflows are only available when the supplemental package is installed, and must be added manually to the Administrator Menu by a Vocera Implementation Engineer.

Workflows	End User	Charge Nurse/Department Secretary	Super User	Administrator User
Messaging				
Message and Alert Tracking and Reporting: Track and run reports on the delivery of messages and alerts to phones. Find and view message and alert deliveries to a mobile device, as well as the delivery history.		Yes	Yes	Yes
Assignment History: View the assignment history.				Yes
Message Tracking: Track the messages that you sent. You can access the delivery history details for personal and group messages sent from your device.	Yes			
Manage Quick Response Favorites: Manage my quick response favorite preferences.	Yes			
Login or Logout of a Phone: Assign or Unassign the current user to a device. You can log in, send a confirmation message, and log out of a device.	Yes			
Manage Presence States: Manage the Presence States available to Users				Yes
Manage User Presence: Manage the XMPP presence of Vocera Users. You can create, edit, and remove the presence states which are presented to XMPP device users.				Yes
Configuration				
Assign User To A Phone: Assign users to a phone. Users can assign themselves and other users to phones, and remove users from phones. By changing your own assignment to a department, you can make assignments in the other departments for which you are responsible.		Yes		

Workflows	End User	Charge Nurse/Department Secretary	Super User	Administrator User
Manage Configurations: Create/remove/edit configurations for a facility. You can define the assignment levels for alert escalation recipients, create one or more configurations using the defined assignment levels, and then associate a configuration with a facility in the network.				Yes
Manage Functional Roles: Manage the functional roles for a facility. You can create, edit, and remove functional roles, as well as deactivate roles, for staffing assignments.				Yes
Manage Locations: You can create, remove, and edit locations for staff assignment.				Yes
Manage Message Quick Responses: You can add, remove, or change pre-defined messages (quick responses) and their categories.			Yes	Yes
Manage Phones: View the phone's current status, assign its default unit, and assign to a user. You can manage phone information for users and default units, list disconnected phones, and view registration history.			Yes	Yes
Monitor Tech				
Manage Monitor Technician: You can create and delete a Monitor Technician, edit the Monitor Technician's identifying number, and assign or change a Monitor Technician's phone association				Yes
Manage Monitor Assignments: You can manage Monitor Technician assignments to patient beds.				Yes
Find Patient and View Department Census: You can view department census, and search	User's unit only	User's unit only	User's unit only	Access all units

Workflows	End User	Charge Nurse/Department Secretary	Super User	Administrator User
for detailed patient information.				