

Vocera Messaging Platform Administration Guide

Version 5.2.3



Notice

Copyright © 2002-2018 Vocera Communications, Inc. All rights reserved.

Vocera® is a registered trademark of Vocera Communications, Inc.

This software is licensed, not sold, by Vocera Communications, Inc. ("Vocera"). The reference text of the license governing this software can be found at <http://www.vocera.com/legal/>. The version legally binding on you (which includes limitations of warranty, limitations of remedy and liability, and other provisions) is as agreed between Vocera and the reseller from whom your system was acquired and is available from that reseller.

Certain portions of Vocera's product are derived from software licensed by the third parties as described at <http://www.vocera.com/legal/>.

Microsoft®, Windows®, Windows Server®, Internet Explorer®, Excel®, and Active Directory® are registered trademarks of Microsoft Corporation in the United States and other countries.

Java® is a registered trademark of Oracle Corporation and/or its affiliates.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owner/s. All other brands and/or product names are the trademarks (or registered trademarks) and property of their respective owner/s.

Vocera Communications, Inc.

www.vocera.com

tel :: +1 408 882 5100

fax :: +1 408 882 5101

Last modified: 2018-11-27 08:41

VMP-523-Docs build 188



Contents

About the Vocera Messaging Platform.....	7
Integration Options.....	7
VMP Architecture.....	8
Getting Started with VMP.....	10
VMP Server Requirements.....	10
Network Access Requirements.....	10
VMP Software Requirements.....	10
VMP System Account Requirements.....	10
Port Requirements.....	11
Installing the VMP Server.....	13
SSL Certificate Validation.....	19
Configuring the VMP License.....	19
Updating the VMP Server.....	20
VMP Cluster Installation.....	22
Installing the VMP Server on the First Node of a Cluster.....	22
Installing the VMP Server on the Second Node of a Cluster.....	22
Updating a VMP Cluster.....	23
About the Standalone VMP Administrator.....	23
Installing the VMP Administrator on a Standalone Computer.....	23
Starting and Stopping the VMP Server.....	25
Setting VMP Server Log File Options.....	25
Changing the SQL Accounts for the VMP Server.....	26
VMP Server Integration.....	30
Vocera Voice Server Integration.....	30
Configuring Vocera Voice Server and VMP.....	30
Enabling Enhanced Vocera Voice Server NIO Tomcat Support.....	33
VCS Users in the Vocera Voice Server.....	34
Address Book Entry Exporting.....	35
Vocera Secure Texting Integration.....	35
Enabling VST Message Exchange.....	35
VST Message Routing.....	37
Configuring VMP for Active Directory.....	37
Engage Integration.....	39
Integrating with the Engage Patient Context Adapter.....	39
Integrating with the AirStrip ONE Platform.....	42
Enabling Engage SOAP Access.....	43
About Importing and Synchronizing.....	48
About Users and Contacts.....	48

Importing Users From Vocera Voice Server.....	49
Importing Users From Active Directory.....	51
Displaying Active Directory Profile Pictures in VCS.....	53
Importing Users From an Excel or CSV File.....	54
Importing Users From SQL.....	56
Specifying Source Importing Options.....	58
Synchronizing Users and Contacts.....	60
Synchronizing Using Vocera UserID and Active Directory.....	66
Importing Contacts From a Source.....	67
Importing Contacts From a Vocera Voice Server Address Book.....	68
Adding a Secondary Source.....	71
User Devices and Client Application Configuration.....	73
Vocera Solution Comparison.....	73
Sending Installation Information to User Devices.....	74
Autoconfiguration of Vocera Collaboration Suite Devices.....	75
Enabling Email Communication.....	75
Updating the APNS Certificates.....	76
About Device Certificates.....	77
Uploading a Device Certificate.....	78
Configuring VCS to Use Vocera Client Gateway.....	79
Vocera Client Gateway Site Awareness.....	80
Wakeup Notifications for VCS Clients.....	80
VCS Wi-Fi Configuration Best Practices.....	81
Wi-Fi Supported Settings.....	81
Site Survey.....	81
Smartphones.....	81
Deployment Models.....	82
WLAN Settings.....	82
Security.....	83
VMP Security.....	85
Configuring the VMP Server For Secure Connections.....	85
Enforcing SSL on the VMP Server.....	86
iOS and Android Security.....	87
Comet Notifications.....	87
Apple iOS Server Data Encryption.....	87
Apple APNS Data Transfer Encryption.....	88
Apple iOS Device Data Encryption.....	88
Android Server Data Encryption.....	89
Android GCM Device Data Encryption.....	90
Enforcing Password Use.....	90
Remote Wipe.....	92
Performing a Remote Wipe from the VMP Administrator.....	92
Performing Remote Wipe Using Microsoft Exchange.....	92
Performing Remote Wipe Using Outlook Web.....	92
Performing Remote Wipe Using a Mobile Device Management Solution.....	92

Performing an Exchange Management Shell Remote Wipe.....	93
High Availability and VMP.....	94
Failover Configuration.....	94
Configuring Failover Email Notifications.....	95
Post Failover Configuration.....	95
Restarting the Primary Server After Failover.....	96
SSL in a VMP Failover Environment.....	96
Using SQL AlwaysOn Availability Groups and Failover Cluster Instances.....	97
Wireless Gateway and Email Configuration.....	99
Wireless Gateway Configuration.....	99
SNPP Gateways.....	99
Configuring WCTP Polling.....	101
Inbound Integration.....	102
WCTP Connections.....	102
SOAP Connections.....	108
Email Monitoring With VMP Messages.....	111
The VMP Administrator.....	115
Logging into the VMP Administrator.....	115
The VMP Administrator Modules.....	116
Users and Groups.....	117
Contacts.....	138
Messaging.....	144
Content.....	164
Reports.....	170
Configuration.....	185
The VMP Web Console.....	192
VMP Web Console Overview.....	192
Browser Requirements.....	192
Logging into the VMP Web Console.....	192
The Monitor View.....	193
Monitor View Features.....	193
Filtering the Monitor View.....	194
Web Console Secure Messages.....	196
Sending a Message from the VMP Web Console.....	196
About Mass Notifications.....	208
Continuing a Message Conversation.....	208
Viewing Participants.....	212
Adding a User to a Message Conversation.....	213
Filtering Message Conversations.....	215
Hiding a Message.....	216
Patient Information and Alarms.....	216
The Patients View.....	221
About User Permissions.....	222
Granting Existing Users Access to the VMP Web Console.....	222
Granting Users Scheduling Permissions.....	224

Allowing Users to View Messages.....	226
On-Call Status and Schedules.....	227
Modifying Your On-Call Status.....	228
Modifying Any On-Call Status.....	229
Creating On-Call Schedules.....	230
Viewing the Schedule Dashboard.....	234
Printing a Schedule.....	236
Web Console Contacts.....	236
Using Web Console Contacts.....	236
Using Web Console Favorites.....	239
Displaying Contacts in Sites.....	240
Calling a Contact.....	241
Changing Your Profile Picture.....	242
Appendixes.....	245
VMP Administrator Configuration Options.....	245
VMP Enterprise Manager Configuration Options.....	250
Frequently Asked Questions.....	254

About the Vocera Messaging Platform

The Vocera Messaging Platform (VMP) provides an enterprise messaging solution designed to address the unique communication challenges of healthcare. Users can leverage the communication capabilities of VMP from the Vocera Collaboration Suite, Vocera Secure Texting, the VMP Web Console, and the Vocera badge.

The VMP platform runs on Windows Server and integrates with Windows SQL Server. User data can be imported from Active Directory, Vocera Voice Server, Vocera Secure Texting, SQL, or Excel/CSV data files.

VMP administrators perform initial system configuration and ongoing system administration. Initial configuration tasks are managed from the VMP Enterprise Manager and the VMP Administrator. Administrative tasks are also managed from the VMP Web Console.

Integration Options

The Vocera Messaging Platform (VMP) runs on Windows Server and integrates with other server systems.

Table 1: Integration options

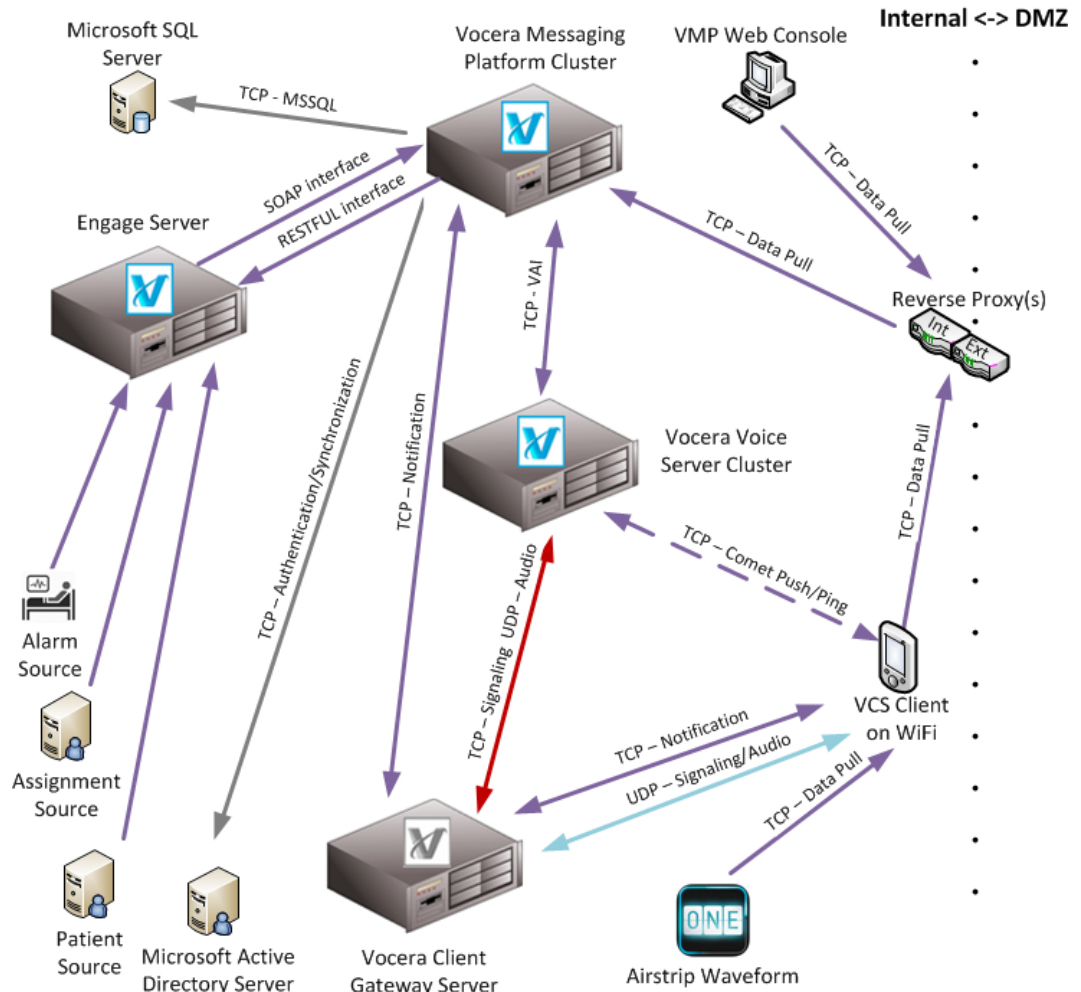
System	Integration Details
Active Directory Server	The VMP Server uses Active Directory to synchronize domain users with the VMP Administrator.
SQL Server	The VMP Server uses SQL Server to store the system data in a secure database. Users and Contacts can also be imported from an SQL database. Vocera highly recommends that you create a unique instance on the SQL Server to house the VMP database. This ensures that resources can be assigned as specified in the Vocera Messaging Platform Server Sizing Matrix .
Apple Push Notification Service (APNS)	The VMP Server integrates with APNS when Apple iOS devices are not connected directly to the Vocera infrastructure to receive direct push notifications. The APNS Servers are not hosted within a network. The VMP Server connects to the APNS network through HTTP(S). The APNS security certificate must be updated every year. The VMP Server will do this automatically for you if possible. See Updating the APNS Certificates on page 76 for details on updating your APNS certificate.
Google Cloud Messaging Service (GCM)	The VMP Server integrates with GCM when Google Android devices are not connected directly to the Vocera infrastructure to receive direct push notifications. The GCM Servers are not hosted within a network. The VMP Server connects to the GCM network through HTTP(S).
Vocera Voice Server	The VMP Server integrates with the Vocera Voice Server through a direct network connection.
Engage Platform	The VMP Server can obtain patient information through the Engage Patient Context Adapter, and can receive alarms through the VMP SOAP interface. These alarms are sent to client devices and the VMP Web Console as notifications.

VMP Architecture

The VMP architecture indicates how the VMP Server is connected to other Vocera servers, to client devices, and to other servers.

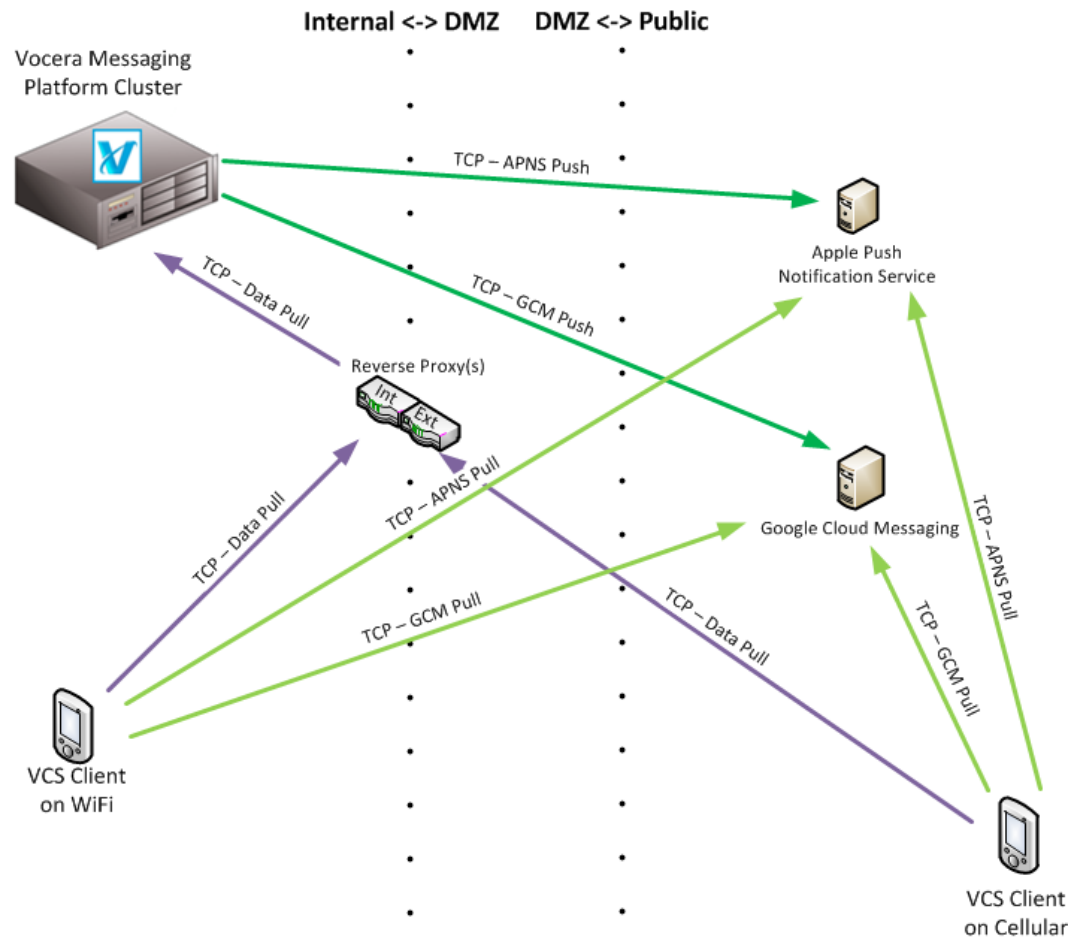
The following diagram shows how the VMP Server connects to other servers inside your network firewall. As shown in the diagram, a reverse proxy can be used to communicate with entities outside of your corporate firewall.

For information on the ports that these connections use, see [Port Requirements](#) on page 11.



Note: In older versions of VMP, devices running the Vocera Collaboration Suite app communicated with the Vocera Voice Server using a Comet connection. This connection option is still available for backward compatibility, but has been replaced by a TCP-based connection to the Vocera Client Gateway server. See [Configuring VCS to Use Vocera Client Gateway](#) on page 79 for more details.

When the Vocera Collaboration Suite app is being used outside of your corporate firewall, it communicates with the Apple Push Notification Service (APNS) if you are using the Apple iOS operating system, or with the Google Cloud Messaging service (GCM) if you are using the Android operating system. The diagram below shows the relationships between the VMP Server, VCS, APNS, and GCM.



Note: For more information on security and the interface to APNS and GCM, see [iOS and Android Security](#) on page 87.

The VMP Server can also use the Vocera Voice Server to communicate with Vocera badges, or to interact with the Vocera SIP Telephony Gateway when VCS apps are making cellular calls.

VMP also has a SOAP-based API that external systems can use to send messages and receive delivery statuses and responses to the messages. See the *Vocera Messaging Platform API Guide* for more information on this API, and also see [SOAP Connections](#) on page 108 for information on how to integrate an inbound SOAP connection to the VMP Server.

VMP also supports WCTP as an inbound and outbound protocol to allow third-party systems to initiate and receive messages. See [WCTP Connections](#) on page 102 for more details.

Getting Started with VMP

Learn about VMP Server system requirements, and learn how to install the VMP Server.

For detailed information on operating system requirements, MS SQL Server requirements, and more, see the [Vocera Messaging Platform Server Sizing Matrix](#).

VMP Server Requirements

Before you begin your installation, make sure that the VMP installation server is running with at least 4 GB RAM and 120 GB HDD and meets the requirements described here.



Note: The VMP Server can be installed on a virtualized server running VMWare. For details about virtualization, see the [Vocera Messaging Platform Server Sizing Matrix](#).

If you are using an SSL connection, the VMP Server must validate the SSL certificate using the existing Windows mechanisms. See [SSL Certificate Validation](#) on page 19 for more details.

Network Access Requirements

Prior to installation, make sure that the minimum network access requirements are met.

Table 2: Network access requirements

Requirement	Details
HTTPS connection	SMS message aggregation requires an outbound HTTPS connection.
IIS Service	The IIS World Wide Web Publishing Service must not be running on port 80 or 443.

VMP Software Requirements

To install and deploy the VMP Server, you must have the required software.

- The VMP installation files and license file.
- An SSL certificate if needed.
- If you are working with the Vocera Voice Server, version 4.4.3 or later is required. If your organization is using Vocera Voice Server departments and synchronizing them with VMP groups, Vocera Voice Server 5.2 or later must be installed.

If you do not have these items ready for your installation, speak with your Vocera services representative before continuing with the installation.

VMP System Account Requirements

During the VMP Server installation, two system accounts are created on the associated SQL Server: `wicapplication` and `wicauth`.

- `wicapplication` is the VMP system application account.
- `wicauth` is the user authentication account.

The accounts are created automatically during platform installation. The installation wizard prompts you for the user ID and password that you use to log in to the SQL server.

Port Requirements

To install VMP, you must configure a firewall or proxy firewall.

This firewall or proxy firewall must be configured with the following conditions:

- Support for resolving Internet addresses that use DNS
- A firewall proxy that does not change incoming or outgoing data (transparent proxy)

To allow communication between VMP devices and services, configure communication protocols and port numbers on the firewall and within the organization network environment.

The following tables describe important system port requirements.

Table 3: Protocol and port requirements for VMP Server


Description	Protocol	Port Number
VMP Server => Microsoft SQL Server	TCP	1433
VMP Web Console Users' computers => VMP Server	TCP	80
VMP Web Console Users' computers => VMP Server	TCP	443 (Using SSL)
VMP Server => Microsoft Active Directory Server	TCP	389
VMP Server => Microsoft Active Directory Server	TCP	636 (using SSL)
VMP Server <=> Vocera Client Gateway Server	TCP	5008
 Note: The Use VCG for VCS client connection management option must be set in the VMP Administrator.		

Table 4: Protocol and port requirements for Apple iOS device messaging

Description	Protocol	Port Number	Destination Host
VMP Server => Apple Push Notification Service (APNS)	TCP	2195 2196	gateway.push.apple.com
VMP Server => Apple Push Notification Service (APNS)	TCP	443	gateway.push.apple.com
Apple iOS devices using Wi-Fi connection => Apple Push Notification Service (APNS)	TCP	5223	gateway.push.apple.com

Table 5: Protocol and port requirements for Google Cloud Messaging (GCM) for Android devices

Description	Protocol	Port Number	Destination Host
VMP Server => Google Cloud Messaging (GCM)	TCP	443	android.googleapis.com
Android devices using Wi-Fi connection => Google Cloud Messaging (GCM)	TCP	5228 5229 5230	Your firewall must accept outgoing connections to all IP addresses contained in the IP blocks listed in Google's ASN of 15169.


 **Note:** Android devices running version 4.3 or later can use port 443 as a fallback if the other three ports are not working.

Table 6: Protocol and port requirements for Simple Network Paging Protocol (SNPP) gateways (using default port)

Description	Protocol	Port Number
VMP Server => SNPP Gateway	TCP	444

Table 7: Protocol and port requirements for Wireless Communications Transfer Protocol (WCTP) gateways (using default ports)

Description	Protocol	Port Number
VMP Server <=> WCTP Gateway	TCP	80
VMP Server <=> WCTP Gateway	TCP	443

Table 8: Protocol and port requirements for Vocera Secure Texting

Description	Protocol	Port Number
VMP Server <=> VST Server	TCP	443

Table 9: Protocol and port requirements for Engage server (using default ports)

Description	Protocol	Port Number
VMP Server => Engage server	REST	80
VMP Server => Engage server	REST	443

Table 10: Protocol and port requirements for email

Description	Protocol	Port Number
VMP Server <=> SMTP	SMTP	25 465 for secure SMTP
VMP Server <=> IMAP	IMAP	143 993 for secure IMAP (IMAP SSL)
VMP Server <=> POP3	POP3	110
VMP Server <=> EWS	Exchange Web Services (EWS)	80 443 for secure EWS

Table 11: Protocol and port requirements for Vocera Collaboration Suite when on premises

Description	Protocol	Port Number
Vocera Collaboration Suite <=> VMP	TCP	443
VCS <=> Vocera Client Gateway signaling	see Port Number	5060-5080 (SIP) If the Use VCG for VCS client connection management option is set, the protocol is TCP. Otherwise, it is UDP.
	UDP	5888-5889 (VOMO)
VCS <=> Vocera Client Gateway audio	UDP	7700-8467 (iPhone) 7700-8467, 32768-65536 (Android)

Description	Protocol	Port Number
VCS <=> Vocera Voice Server Ping/Comet connection This is used if the Use VCG for VCS client connection management option is not set in the VMP Administrator.	TCP	8080 if Enable Enhanced Voice Server NIO Tomcat Feature option is set in the VMP Administrator 80/443 if Enable Enhanced Voice Server NIO Tomcat Feature option is not set in the VMP Administrator

Table 12: Protocol and port requirements for Vocera Collaboration Suite when off premises

Description	Protocol	Port Number
Vocera Collaboration Suite <=> VMP	TCP	443

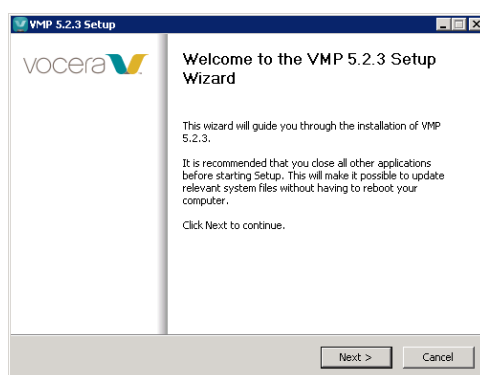
Installing the VMP Server

VMP is shipped with a setup file that enables you to install the VMP Server. Before you can install this setup file, you must disable the IIS World Wide Web Publishing Service.

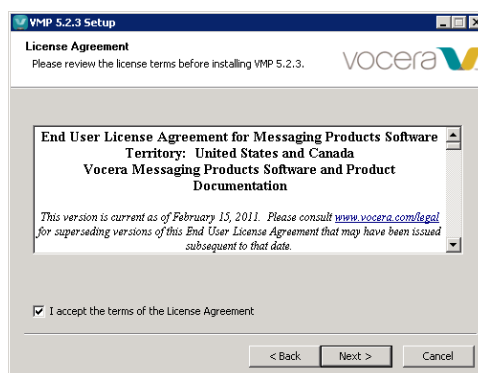


Note: If you are using an SSL connection, the VMP Server must validate the SSL certificate using the existing Windows mechanisms. See [SSL Certificate Validation](#) on page 19 for more details.

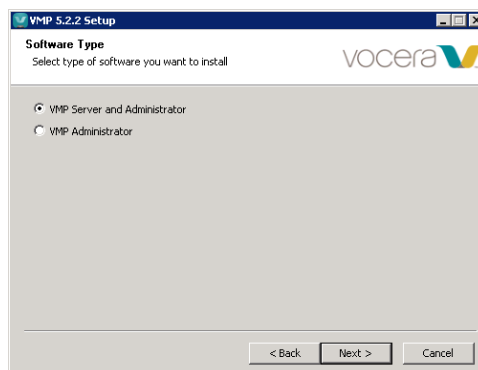
- Use the following steps to turn off the IIS World Wide Web Publishing Service. This step ensures that port 80 is open for the VMP Web Console.
 - Open the Windows Services application:
Windows > Start > Administrative Tools > Services
 - Click to select World Wide Web Publishing Service.
 - Right-click and select Properties.
 - From the Startup type dropdown list, select Disabled.
 - Click Stop, and click Apply.
- Execute the VMP setup file on the VMP installation server.
- In the Welcome screen, click Next.



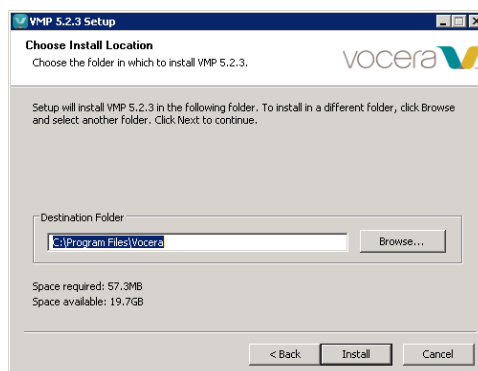
- Accept the License Agreement, and click Next.



5. In the Software Type dialog, select VMP Server and Administrator, and click Next.



6. In the Destination Folder field, Vocera recommends that you use the default destination folder provided. To use a different destination folder, type or browse for the folder in which the VMP Server is to be installed, and click Install. You may need to wait a few moments while the installation process initializes and copies files.



7. In the Create VMP Database Wizard dialog, do the following:
 - a. In the SQL Server field, enter the SQL Server VMP instance name using the format of ServerName\InstanceName.



Tip: Vocera recommends that you type the name of the Server and instance name instead of using the dropdown list.

- b. Select the Sql Server Authentication radio button.
- c. Enter the server authentication Login and Password.
- d. Click Next.



Note: For details about the SQL Server requirements, see the [Vocera Messaging Platform Server Sizing Matrix](#).

8. Enter a password for the wicapplication and wicauth accounts using the following rules, and click Next.

Passwords must be a minimum of 7 characters and include at least three of the following:

- Uppercase letter
- Lowercase letter
- Symbol and/or number



Note: Do not change the system account names.

9. In the VMP system Settings dialog, enter the VMP Server public and internal host information, and the SMTP settings as shown in the table below.

Table 13: VMP SMTP settings

Setting	Description
Mail Server	The Exchange server name or IP address.
Mail Server Port	The port on which the Exchange server resides.
Email Address	The email address for sending out installation communications and receiving server status updates.
Use Authentication	Enable the Use Authentication checkbox and enter the credentials, as these credentials are required to access the Exchange server.

Click Complete.



Tip: Use the DNS name for the external host name to make IP scheme updates easier. If configuring a device manually, use an IP address.

10. If the VMP Server is using a Vocera Voice Server:

- a. Select [Integrate with Voice Server](#).
- b. In the [Active Voice Server IP](#) field, type the IP address of the Voice server that you want to use. If you are using a clustered environment, ensure that the IP address of the active Voice server is listed first.

- c. In the **Port** field, specify the port number that the Voice server is using. In most environments, you can use the default port number that is provided in the installer.
- d. Select **Use SSL Authentication** if you are using SSL when communicating with the Voice server.

Click **Next**. If you have enabled integration with a Vocera Voice Server, the VMP installer checks that the connection to the Vocera Voice Server is working properly.



Note: To fully integrate the VMP Server with the Vocera Voice Server, you must configure the Vocera Voice Server for use with VMP and synchronize the Vocera Voice Server with the VMP Server. See [Vocera Voice Server Integration](#) on page 30 and [Importing Users From Vocera Voice Server](#) on page 49 for more details.

11. If the VMP Server is using an Active Directory server:

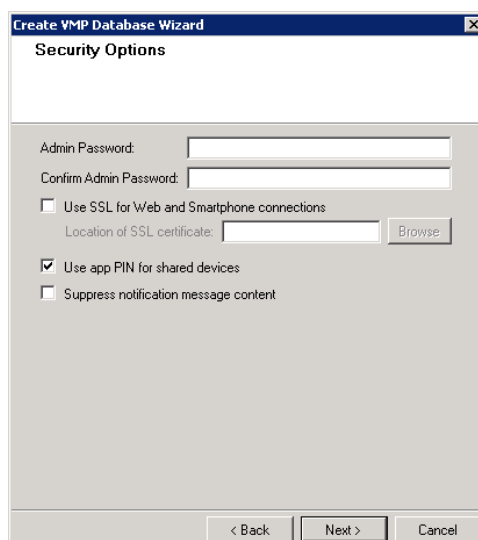
- a. Select **Integrate with Active Directory**.
- b. In the **Server Name or IP** field, type the domain name or the IP address of the Active Directory server that you want to use.
- c. Select **Use Active Directory for Authentication** if you want to authenticate using Active Directory usernames and passwords. The default is to use VMP Server authentication.
- d. Select **Use SSL Authentication** if you are using SSL when communicating with the Active Directory server.

Click **Next**. If you have enabled integration with an Active Directory server, the VMP installer checks that the connection to the Active Directory server is working properly.



Note: To fully integrate the VMP Server with the Active Directory server, you must synchronize the Active Directory server with the VMP Server. See [Importing Users From Active Directory](#) on page 51 for more details.

12. In the **Security Options** window:



- a. In the Admin Password field, type the password to use for the default administrator account.
- b. In the Confirm Admin Password field, retype this password.
- c. Select **Enforce SSL for Web and Smartphone connections** to enforce the use of secure connections.
- d. If **Use SSL for Web and Smartphone connections** has been selected, in the **Location of SSL certificate** field, specify the location of the SSL certificate to use with this installation. Click **Browse** to display the certificates that are available to you.
- e. Select **Use app PIN for shared devices** if you want to force users to supply a PIN when accessing this server from the Vocera Collaboration Suite. This sets the **Enforce App PIN** configuration option to **SHARED**. If this checkbox is not selected, **Enforce App PIN** is set to **OFF**.



Note: You can override this specification for any individual user. See [Editing User Information](#) on page 122 for more details.

- f. You do not need to select the **Suppress notification message content** option, as message content is now no longer displayed in notifications.
- g. Click **Next** to continue.



Tip: Vocera recommends that you use SSL to transmit information. If you are using VMP to transmit confidential patient information, your jurisdiction may require by law that this information be transmitted securely.

13. The installer creates the VMP databases on the SQL server. When the script is complete, click **OK**.
 14. This release opens the VMP Enterprise Manager after the database script is complete. Normally, you do not need to make any changes to the VMP configuration at this point. See [VMP Enterprise Manager Configuration Options](#) on page 250 for details on the VMP Enterprise Manager configuration options.
 15. Close the application to complete the installation process. The installer VMP now starts the Vocera Data Exchange service (referred to as WDE here).
 16. Click **Finish** to close the installer.
 17. The VMP Server is now installed. Confirm a good installation by opening a supported Web browser and pointing to the server URL. If VMP is installed correctly, the VMP Web Console opens at the login page.
- For information on supported Web browsers, see [Browser Requirements](#) on page 192.

SSL Certificate Validation

The VMP Server must validate any SSL certificate using the existing Windows mechanisms before it will allow an HTTPS connection to a remote system.

The VMP Server now enforces the following requirements:

- The certificate subject name must match the domain name used for the connection.
- Self-signed certificates must be in the VMP Server's Windows key store.
- If you are using your own internal certificate authority to sign the certificate, the internal CA's certificate must be in the VMP Server's Windows key store.
- If the certificate uses an IP address, the connection configuration must use an IP address. Similarly, if the certificate uses a DNS name, the connection configuration must use the same DNS name.

This certificate requirement affects certificates defined for use on the Vocera Voice Server.

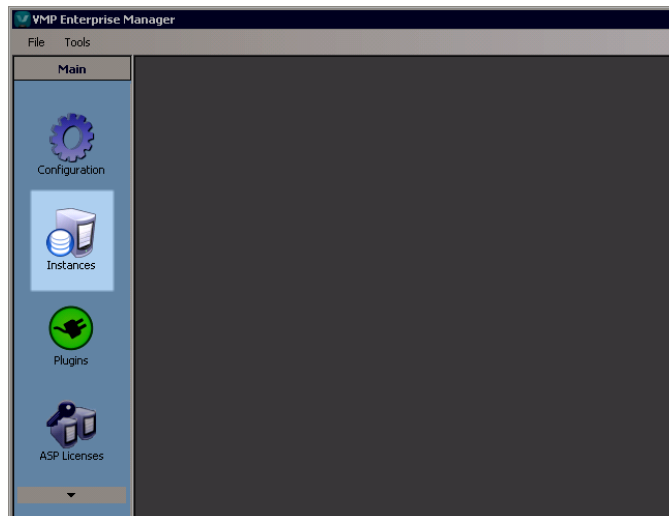


Note: Vocera Collaboration Suite clients and VMP Web Console clients are not affected by this behavior.

Configuring the VMP License

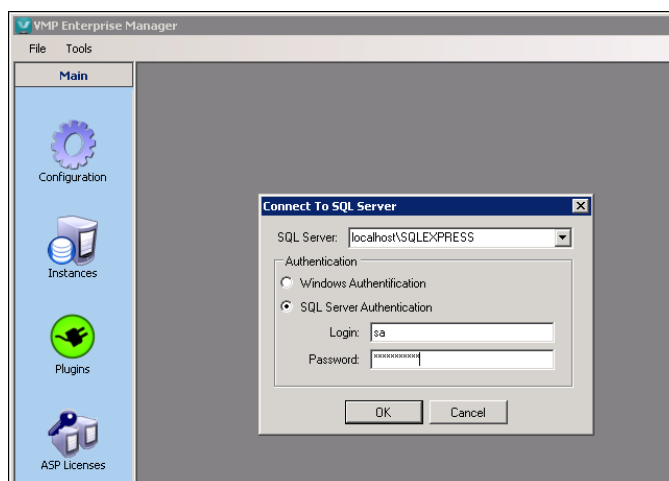
Before you can use the VMP Server, you must install a valid license. You can do this from the VMP Enterprise Manager.

1. Start the VMP Enterprise Manager application:
All Programs > VMP > VMP Enterprise Manager
2. Click the Instances icon.



The Connect To SQL Server dialog box appears.

3. Type the SQL Server administrator credentials.

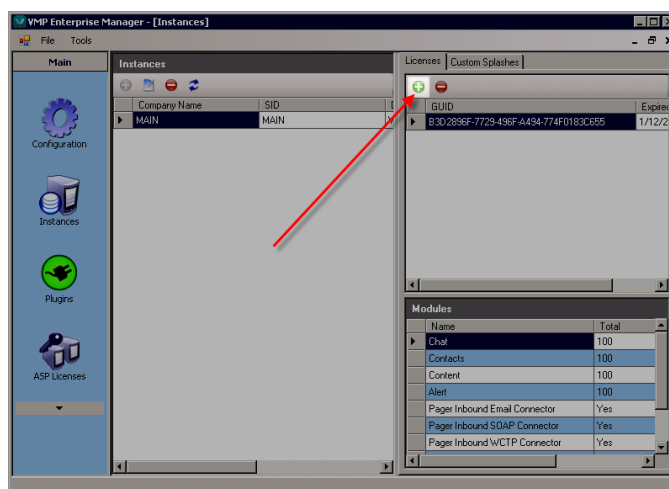


The Instances window appears.



Note: For more information about the SQL Server credential requirements, see the [Vocera Messaging Platform Server Sizing Matrix](#).

4. In the Licenses tab, select the Install License button.



5. Navigate to the license file and click Open.



Note: The license file is provided by the Vocera order management team. The file is distributed as a zip file. Extract the file before you begin the installation to import the WLC extension.

6. Click OK to close the install dialog.

The Modules panel displays the details of your license. In particular, note that the Pager Inbound Email Connector, Pager Inbound SOAP Connector, and Pager Inbound WCTP Connector fields specify whether your VMP Server is licensed to use any of the inbound Email, SOAP, and WCTP connections, respectively. These fields are set to Yes only if your license has enabled them. See [Inbound Integration](#) on page 102 for more information on inbound connections.

Updating the VMP Server

If you have previously installed the VMP Server, you can use the VMP setup file to upgrade your installation to the latest version.



Important: If you are currently running version 4.9.x of the Vocera Messaging Platform, you must first upgrade to version 5.1 or 5.2 before upgrading to version 5.2.3. You cannot upgrade directly from version 4.9.x to version 5.2.3.



Note: For best results, save a backup of the contents of the folder in which the VMP Server is installed (by default, this is \Program Files\Wallace), and save a copy of the WICMASTER SQL database.

If you are using an SSL connection, the VMP Server must validate the SSL certificate using the existing Windows mechanisms. See [SSL Certificate Validation](#) on page 19 for more details.

1. Stop the Vocera Data Exchange service. See [Starting and Stopping the VMP Server](#) on page 25 for details on how to do this.
2. Execute the updated VMP setup file on the VMP installation server.
3. In the Welcome screen, click **Next**.
4. Accept the License Agreement, and click **Next**.
5. In the Software Type dialog, select **VMP Server and Administrator**, and click **Next**.
6. Accept the existing Destination Folder and click **Install**.
7. In the Create VMP Database Wizard dialog, do the following:
 - a. Ensure that the SQL Server field contains the SQL instance name that the VMP Server is using.

- b. Select the **Sql Server Authentication** radio button.
- c. Enter the server authentication **Login** and **Password**.
- d. Click **Next**.



Note: For details about the SQL Server requirements, see the [Vocera Messaging Platform Server Sizing Matrix](#).

8. Click **OK** to confirm that the existing database will be upgraded.
9. The database wizard now enables you to change the SQL login names that VMP uses. You do not normally need to change these login names. Click **Next**.
10. The installer will upgrade the VMP databases on the SQL server. When the script is complete, click **OK**.
11. If the VMP Enterprise Manager opens after the database script is complete, close the application to complete the installation process. Click **Finish** to close the installer.
12. Restart the server.
13. The VMP Server is now updated. Confirm a good installation by opening a supported Web browser and pointing to the server URL. If VMP is installed correctly, the VMP Web Console opens.

VMP Cluster Installation

To ensure maximum reliability, you can set up a cluster and install the VMP Server on each node of the cluster.

For more information on using the Vocera Messaging Platform in a clustered environment, see [High Availability and VMP](#) on page 94.

Installing the VMP Server on the First Node of a Cluster

When installing the VMP Server in a clustered environment, the first step is to install on the first node of the cluster.

1. Perform a normal installation of the VMP Server using the steps in [Installing the VMP Server](#) on page 13.
2. Test your installation to ensure the server is working properly.
3. Copy the server configuration file, **WIC.config**, to a folder that the second node of the cluster can access.



Note: The **WIC.config** file is located in the VMP installation folder. By default, this is `\Program Files\Vocera\WIC`.

Installing the VMP Server on the Second Node of a Cluster

After you have installed the VMP Server on the first node of a cluster, you can use the configuration file from this node when installing on the second node of the cluster.

1. Create the VMP installation folder for the VMP Server. By default, the path is:
`\Program Files\Vocera\WIC`
2. Locate the copy of the server configuration file, **WIC.config**, that you created when installing the VMP Server on the first node of the cluster. Copy this file to the VMP installation folder that you have just created.
3. Turn off the IIS World Wide Publishing Service. See [Installing the VMP Server](#) on page 13 for instructions on how to do this.
4. Execute the VMP setup file.
5. Accept the License Agreement, and click Next.
6. In the Software Type dialog, select VMP Server and Administrator, and click Next.
7. In the Install Location field, enter the path of the installation directory into which you copied the **WIC.config** file. Click Install.
8. At the Create VMP Database Wizard prompt, confirm that the SQL Server name is correct.



Note: The SQL Server name is supplied by the **WIC.config** file that you copied.

9. Select the Sql Server Authentication radio button, and enter the SA Login and Password. Click Next.
10. When prompted, click OK to upgrade the database.
11. Leave the SQL Account Configuration page unchanged and click Next.



Note: The account configuration information is supplied from the **WIC.config** file that you copied. Do not change this information.

12. Complete the VMP System Setting dialog and all subsequent steps in the Create VMP Database Wizard as described in [Installing the VMP Server](#) on page 13.

Updating a VMP Cluster

If you are using the VMP Server in a clustered environment and you want to install an update, you must update the VMP Server on each node of the cluster.



Important: If you are currently running version 4.9.x of the Vocera Messaging Platform, you must first upgrade to version 5.1 or 5.2 before upgrading to version 5.2.3. You cannot upgrade directly from version 4.9.x to version 5.2.3.

1. Stop the Vocera Data Exchange Service on both nodes of the cluster.
2. On the first node of the cluster, follow the instructions in [Updating the VMP Server](#) on page 20 to update the VMP Server.
3. The upgrade installer automatically starts the Vocera Data Exchange Service on the first node of the cluster. Stop the Vocera Data Exchange Service on the first node of the cluster before proceeding.
4. On the second node of the cluster, follow the instructions in [Updating the VMP Server](#) on page 20 to update the VMP Server.
5. Restart the Vocera Data Exchange Service on both nodes of the cluster.

About the Standalone VMP Administrator

The VMP Administrator can be installed on a server other than the VMP Server. It can also be installed on the administrator's personal computer.

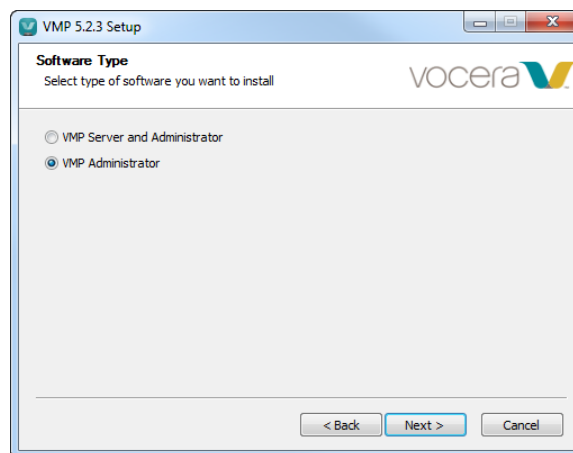
To use the VMP Administrator on a standalone computer, you must have the following:

- The installation disk or folder that you used to install the VMP Server.
- The SQL server name and instance name.
- Remote connections enabled on the SQL server.
- The login password for the `wicauth` account on the SQL server.
- The Active Directory server IP address.

Installing the VMP Administrator on a Standalone Computer

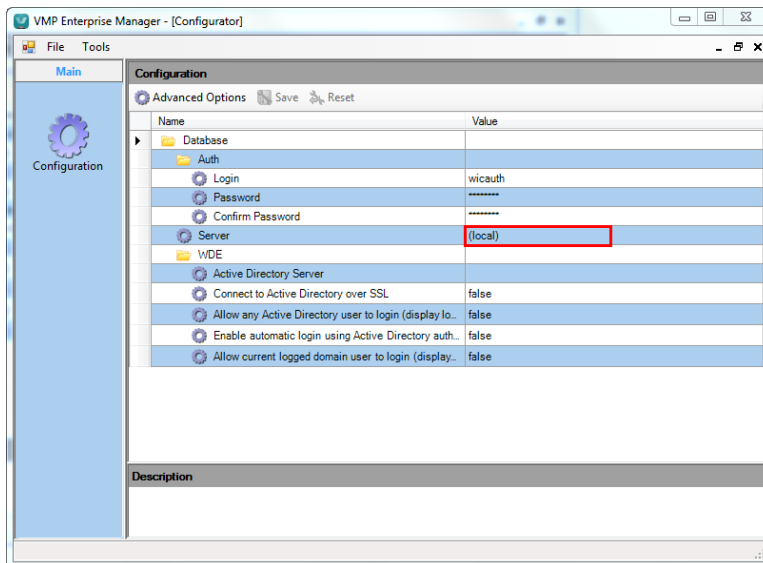
You can use the VMP installation setup file to install the VMP Administrator on a computer other than the one on which the VMP Server is installed.

1. Locate the installation disk or folder that was used to install the VMP Server. In this folder, start `Setup.exe` on the desired computer.
2. Accept the license agreement and click Next.
3. In the Software Type dialog box, select VMP Administrator. Click Next.

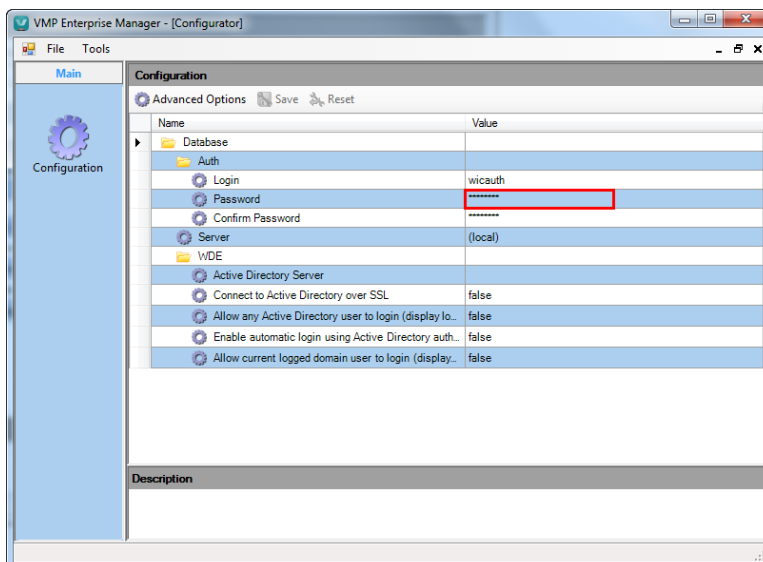


4. Accept the default Destination Folder, or click Browse to select a custom installation folder, then click Install.

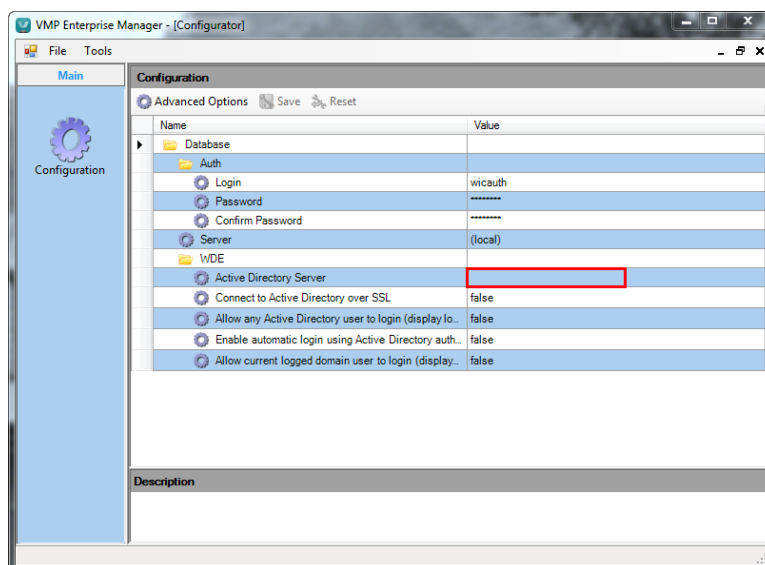
- In the VMP Enterprise Manager Configuration window, in the Server row, type the location of the SQL server that the VMP Server is using. This consists of the IP address or name of the computer that the SQL server is on, followed by a backslash, followed by the name of the SQL server (for example, MYCOMPUTERNAME\SQLSERVERNAME).



- In the Auth section, in the Password field, type the password for the wicauth account on the SQL server. This account was created when the VMP Server was installed.



- In the Confirm Password field, retype the password for the wicauth account.
- In the WDE section, in the Active Directory Server row, type the IP address for the Active Directory server.



9. Click Save and close the VMP Enterprise Manager.
10. Click Finish.

If you are installing a standalone VMP Administrator to work with a running VMP Server, you will need to configure your Vocera Voice Server to add this new installation to the list of recognized VMP IP addresses. See [Configuring Vocera Voice Server and VMP](#) on page 30 for details.



Note: If the standalone VMP Administrator does not start properly after you have installed it, ensure that the connection to the SQL server is working properly.

Starting and Stopping the VMP Server

When you install the VMP Server, it is automatically started for you. To restart the server, you must restart the Vocera Data Exchange service.

Like any other service running on Windows, the Vocera Data Exchange service can be stopped, started, or restarted.

1. Open the Windows Services application:
Windows > Start > Administrative Tools > Services
2. Click to select Vocera Data Exchange Service.
3. Right-click and select one of the following:
 - Start: start the Vocera Data Exchange service.
 - Stop: stop the service.
 - Restart: restart the service.

Setting VMP Server Log File Options

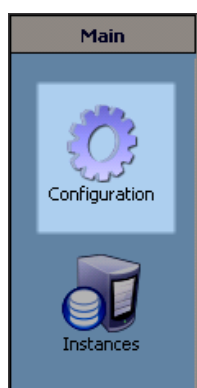
The VMP Server log files provide information on actions performed by the VMP Server. This can be useful if an unexpected error occurs. You can control what goes into these log files.

The server log files are stored in the **WIC\Logs** subfolder of the folder in which the VMP Server is installed. By default, this is **C:\Program Files\Vocera\WIC\Logs**.

You can use the VMP Enterprise Manager to specify what message levels are to appear in log files.

1. From the VMP Server, start the VMP Enterprise Manager.
Start > All Programs > VMP > VMP Enterprise Manager

2. Select Configuration .



The Configuration window appears.

3. Scroll down to the Logging section.
4. Click in the Value column of the Limit log messages to VMP Log File field. From the dropdown list that appears, select one of the following:

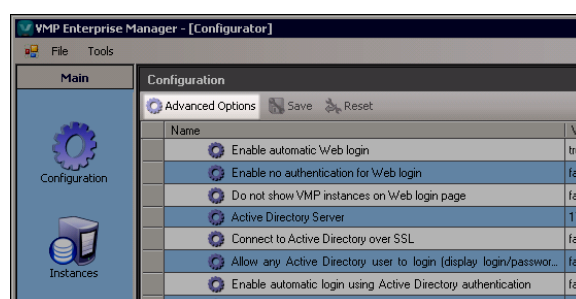
Table 14: Logging options

Option	Description
Do not log	Do not write to the log files.
Write all events	Keep a record of all VMP Server events.
Warnings and Errors	Write only warnings and errors to the log files.
Errors	Write only errors to the log files.

5. Click Save to save your change.



Important: In a live environment, you should not set **Limit log messages to VMP Log File** to **Write all events** and set **Enable extended communication logging** to **true**, as this may cause patient-sensitive data to be written to the log files. The **Enable extended communication logging** setting appears when you click **Advanced Options**.

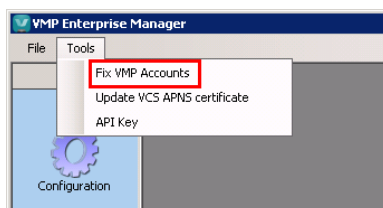


In the event of a failover scenario, the VMP Server log files include a log entry describing the failover to a standby server and the startup details for the new active node. For more information on clustered environments and failover, see [High Availability and VMP](#) on page 94.

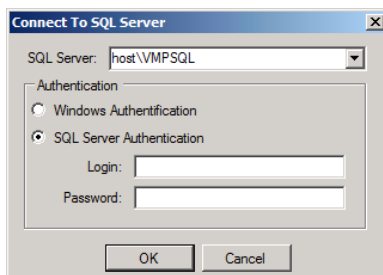
Changing the SQL Accounts for the VMP Server

If the SQL Server database has been updated, and some or all of the SQL accounts that the VMP Server uses have been removed, you can update the VMP Server to use the changed accounts.

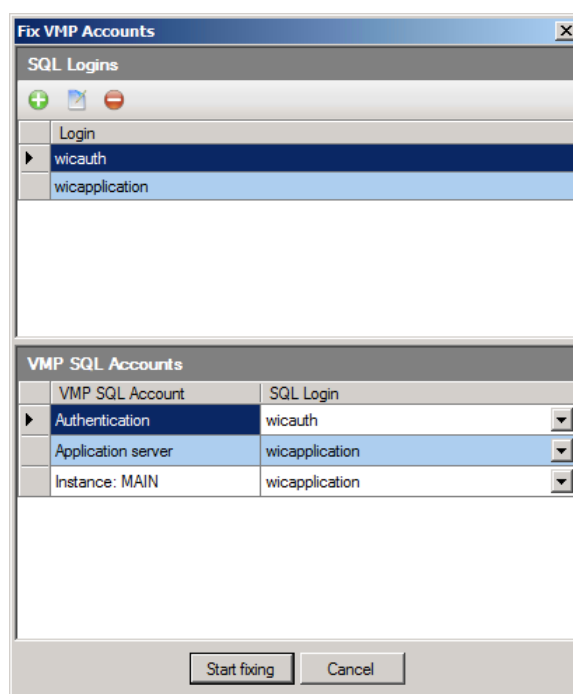
1. Start the VMP Enterprise Manager.
2. From the Tools menu, select Fix VMP Accounts.



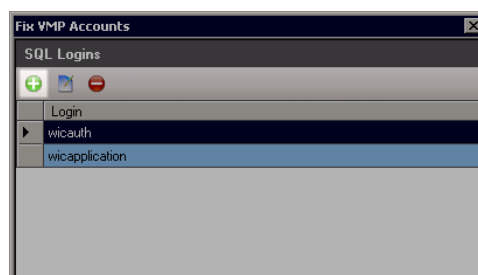
3. In the Connect To SQL Server dialog box, supply the SQL Server authentication:



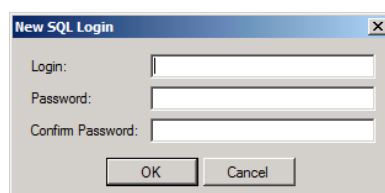
- a. Select the authentication method to use by selecting either Windows Authentication or SQL Server Authentication.
- b. If you have selected SQL Server Authentication, enter your SQL login and password in the Login and Password fields.
- c. Click OK. The Fix VMP Accounts window appears.



4. To add a new SQL account:
 - a. Click Add.

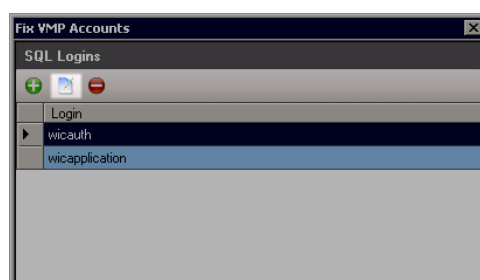


The New SQL Login dialog appears.



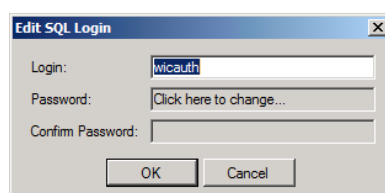
The 'New SQL Login' dialog box contains three text input fields labeled 'Login:', 'Password:', and 'Confirm Password:'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

- b. In the Login field, type the new SQL account name.
 - c. In the Password field, type the password for the new SQL account.
 - d. In the Confirm Password field, retype the password for the account.
 - e. Click OK.
5. To edit an SQL account:
- a. Highlight the account that you want to edit, and click Edit.



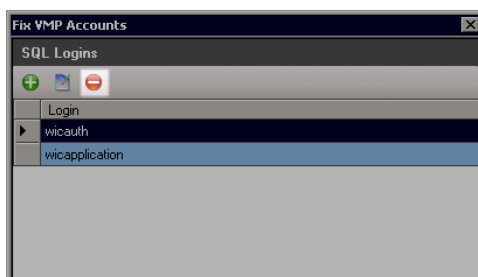
The 'Fix VMP Accounts' dialog box shows a list of 'SQL Logins'. The list includes 'wicauth' and 'wicapplication'. The 'wicauth' entry is highlighted. Above the list are icons for adding (+), deleting (-), and editing (pencil).

The Edit SQL Login dialog appears.



The 'Edit SQL Login' dialog box shows the 'Login' field with 'wicauth' entered. The 'Password' field has a button that says 'Click here to change...'. The 'Confirm Password' field is empty. At the bottom are 'OK' and 'Cancel' buttons.

- b. In the Login field, edit the SQL account name if needed.
 - c. In the Password field, type the new password for the SQL account.
 - d. In the Confirm Password field, retype the new password.
 - e. Click OK.
6. To delete an SQL account, highlight the account that you want to delete, and click Delete.



This is another view of the 'Fix VMP Accounts' dialog box, showing the 'SQL Logins' list with 'wicauth' and 'wicapplication'. The 'wicauth' entry is highlighted.

In the confirmation dialog box that appears, click Yes.

7. To change a VMP SQL account, in the VMP SQL Accounts pane, select the account that you want to change:
- Authentication: The user authentication account.
 - Application server: The VMP system application account.
 - Instance: name: The account that you use to log in to the VMP Server database named name. A standard installation of the VMP Server has a database named MAIN.

From the dropdown list in the SQL Login column, select the VMP SQL account that you want to use.

8. Click **Start fixing**. This runs a script that updates your SQL database. The progress of the script is displayed in a dialog box.
9. When the script has completed, click **OK** to close the display window.

VMP Server Integration

After you have installed the VMP Server, you must integrate it with the other Vocera products and servers in your environment.

Vocera Voice Server Integration

Vocera Voice Server to VMP integration enables Vocera Collaboration Suite users to make Calls and use other Vocera Voice Server capabilities from their devices.



Note: Vocera Voice Server is integrated with the platform as a connector and no additional licensing is required.

To configure the VMP Server to integrate with Vocera Voice Server, prepare the following:

Table 15: Vocera Voice Server configuration requirements

Configuration Requirement	Description
Vocera Voice Server Software Requirements	See VMP Software Requirements on page 10 for information on software requirements.
Vocera Voice Server Credentials	You must have administrator access to the Vocera Voice Server.
VMP Server IP Address	You must have the VMP Server IP address.
Vocera User Email Address	Make sure that each Vocera Voice Server user profile includes the user email address.

The following Vocera Voice Server components must be installed to use the VMP Server with Vocera Collaboration Suite:

- Vocera Client Gateway: required for Wi-Fi calling
- Vocera SIP Telephony Gateway: required for cellular calling

Configuring Vocera Voice Server and VMP

To configure the Vocera Voice Server and VMP to work together, you must access the Vocera Voice Server Administration Console and the VMP Administrator to make the necessary changes.

1. Open the Vocera Voice Server Administration Console.
2. Log on with your administrator credentials.
3. Select the [System](#) view.
4. Select the [License Info](#) tab.

5. In the VAI Application IP Addresses field, type the VMP Server IP address. For load balanced environments, use comma-separated values.

If you have installed the standalone VMP Administrator on a separate computer, and you want to synchronize the VMP Server and Vocera Voice Server from this computer, you must add this computer's IP address to the list.



Note: If you are using other VAI applications, the IP address for VMP must be the first IP address listed in the VAI address field.

6. Click Save Changes.
7. Click the Preferences tab.
8. If the Enable Auto-Logout Period checkbox is selected, set the auto-logout period to a value greater than 1 Minute. This ensures that clients that use the iOS operating system are not unexpectedly logged out.

9. Select the Enable VMP checkbox.

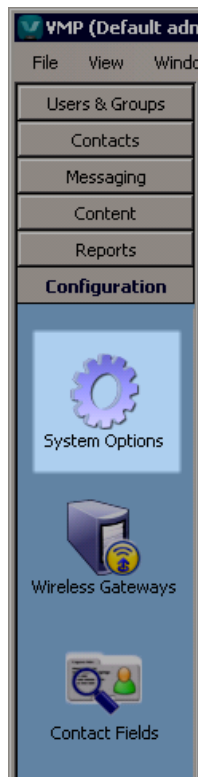
10. Click Save Changes.

11. Start the VMP Administrator:

All Programs > VMP > VMP Administrator

12. In the VMP Login dialog, type **admin** and the password for the administrator account, and click OK.

13. Select Configuration > System Options.



The System Options dialog box appears.

14. Scroll down the System Options dialog box to the Vocera Voice section.

 The screenshot shows the "System Options" dialog box. It has a title bar with "System Options" and a close button. The dialog is divided into several sections. The "Integrations" section is expanded, and the "Vocera Voice" subsection is highlighted with a red border. The "Vocera Voice" section contains the following fields:

Field	Value
Enabled	No
Organization Name	
Text	
Web Console Date Format	MMM/dd/yyyy
Enabled	Yes
Enabled	Yes
IP Addresses	172.30.49.161
Port	80
Use HTTPS	No
VCG IP Addresses	172.30.49.164
VMI Message Expiry (in minutes)	5
Enable Enhanced Voice Server NIO Tomcat Feature	No
Use VCG for VCS client connection management	No

 Below the "Vocera Voice" section is the "Patient Context" section, which includes:

Field	Value
Enabled	Yes
Adapter URI	http://172.30.48.20

 At the bottom of the dialog is a "Description" section with a text area. At the very bottom are three buttons: "OK", "Cancel", and "Help".

15. If you specified the IP address of the Vocera Voice Server that your VMP Server is integrated with during Vocera Messaging Platform installation, the fields in this section are already filled in. If you have not previously specified a Vocera Voice Server, enter the following values:

Table 16: System option configuration values

Option	Value
Enabled	Select Yes from the dropdown list to enable the use of the Vocera Voice Server with the VMP Server.
IP Addresses	Enter the Vocera Voice Server IP address. This can be set in the Voice Server dialog box during installation. See Installing the VMP Server on page 13 for more details. If you are using more than one Vocera Voice Server in a clustered environment, separate the IP addresses with commas, and ensure that the active Vocera Voice Server is listed first.
Port	Enter the Vocera Voice Server port number. The default port number is 80.
Use HTTPS	Select Yes or No from the dropdown list as appropriate for your deployment.
VCG IP Addresses	The Vocera Client Gateway IP address, or comma-separated addresses if the Vocera Client Gateway is operating in a clustered environment. These addresses are configured when the Vocera Voice Server is installed and has been synchronized with the VMP Server, and cannot be edited here.
VMI Message Expiry	The number of minutes before VMI (Vocera Messaging Interface) messages sent from the Vocera Voice Server expire.
Enable Enhanced Voice Server NIO Tomcat Feature	Whether to enable support for scaling changes included in the Vocera Voice Server. Ensure that this feature is enabled in the Vocera Voice Server before enabling it in the VMP Server. See Enabling Enhanced Vocera Voice Server NIO Tomcat Support on page 33 for more details.
Use VCG for VCS client connection management	Whether VCS is to use TCP to communicate with the Vocera Client Gateway server instead of using Comet to communicate with the Vocera Voice Server. See Configuring VCS to Use Vocera Client Gateway on page 79 for more details.

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

After you have configured the Vocera Voice Server and VMP to work with one another, the next step is to import the Vocera Voice Server contacts into the VMP Server. See [Importing Users From Vocera Voice Server](#) on page 49 for information.

Enabling Enhanced Vocera Voice Server NIO Tomcat Support

If your Vocera Voice Server has enabled Non-Blocking I/O (NIO) connectivity with Tomcat, you can configure VMP to use it.

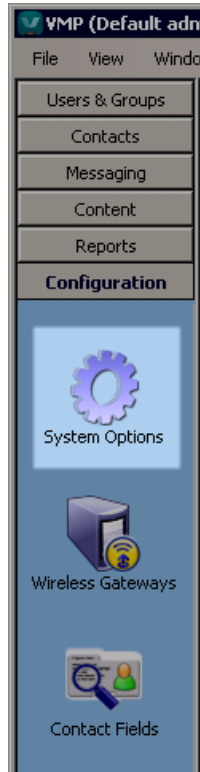
This allows more than 2000 simultaneous Vocera Collaboration Suite clients to connect.



Important: When this capability is enabled, Vocera Collaboration Suite clients connect to the Vocera Voice Server on a different port. The connection is on port 8080, unless you have manually edited the VMP Server configuration to use some other port. (Normally, Vocera Collaboration Suite clients connect to the Vocera Voice Server on port 80 if SSL is disabled, or port 443 if SSL is enabled.) This port change could affect connectivity if you are filtering traffic between the wireless VLAN used by VCS clients and the Vocera Voice Server.

To enable enhanced Vocera Voice Server NIO Tomcat support:

1. Start the VMP Administrator.
2. Select Configuration > System Options.



The System Options dialog box appears.

3. Scroll down to the Integrations > Vocera Voice section.
4. Set the Enable Enhanced Voice Server NIO Tomcat Feature option to Yes.

 The screenshot shows the 'System Options' dialog box. It has a title bar with a close button. The dialog is divided into several sections. The 'Integrations' section is expanded, showing the 'Vocera Voice' subsection. Within this subsection, the 'Enable Enhanced Voice Server NIO Tomcat Feature' option is highlighted with a red box and set to 'Yes'. Other options in the Vocera Voice section include 'Enabled' (Yes), 'IP Addresses' (172.30.49.161), 'Port' (80), 'Use HTTPS' (No), 'VCG IP Addresses', and 'VMI Message Expiry (in minutes)' (5). Below this is the 'Patient Context' section with 'Enabled' (Yes), 'Adapter URL', and 'Adapter Authentication Key'. At the bottom, there is a 'Description' section with a text area containing a warning message about scaling changes. The dialog ends with 'OK', 'Cancel', and 'Help' buttons.

5. Click OK to save your change.

VCS Users in the Vocera Voice Server

When you are creating Vocera Collaboration Suite users, you must create them as Vocera Voice Server users, not as Vocera Voice Server address book entries.

This ensures that the Vocera Collaboration Suite users will have voice capabilities.

Address Book Entry Exporting

When importing users into VMP from an external source, you can create a spreadsheet of address book entries to be exported to the Vocera Voice Server.

This enables badge and Vocera Collaboration Suite users to contact these imported users using the Vocera Voice Server voice recognition capability (the Genie).

To export address book entries to the Vocera Voice Server, select the **Export Address Book Entries to Vocera** checkbox when synchronizing users in the VMP Administrator.



Note: If a VMP user is using the Vocera Collaboration Suite client and wants to use the Genie from this client, this user must also be a Vocera Voice Server user, not a Vocera Voice Server address book entry.

Vocera Secure Texting Integration

Vocera Secure Texting integrates with Vocera Voice Server to supplement the VS voice communication and workflow features with text messaging capabilities. If your Vocera Voice Server is already integrated with the Vocera Messaging Platform, the VST integration extends the reach of your VMP messaging capabilities to include employees of your affiliated organizations.

At the end of the integration of the on-premises Vocera Voice Server with the VST cloud platform:

- Your on-premises badge and VCS users will appear properly in the VST *Directory*, allowing VST users to send messages to them. VST users in your own organization and also your affiliated hospitals and practices appear in the VST *Directory* as well.
- Both your internal VST users and also the users of your affiliated hospitals and practices appear properly in the *Contacts* list of the VCS app, if you have the VMP integration. Badge users and your organization's VCS users continue to appear in the VCS *Contacts* list as well.
- The messaging and voice capabilities of your on-premises solution are integrated with the VST messaging and basic voice capabilities of the cloud platform.



Important: VST 2.1 or later is required.

Enabling VST Message Exchange

You can configure the VMP Server to enable messages and images to be exchanged between Vocera Collaboration Suite users and VST users.

When this capability is enabled, VST users are automatically imported from the VST cloud server into the VMP Server.



Important: VST 2.1 or later is required. If you have previously installed the VST Sync Connector in your on-premises network, you must uninstall it before enabling VST message exchange on the VMP Server. See the *VST Hospital Administrator Guide* for information on upgrading existing VST integrations.

1. Start the VMP Administrator.
2. Select **Configuration > System Options**.



The System Options dialog box appears.

3. Scroll to the Integrations section, and then to the Vocera Secure Texting App - Message Exchange subsection.
4. Set the Enabled field to Yes.

 A screenshot of the 'System Options' dialog box. It contains a list of configuration items in a table-like format. The 'Vocera Secure Texting App - Message Exchange' section is expanded, and the 'Enabled' field is set to 'Yes' (highlighted with a red box). Other fields include 'Adapter URL', 'Adapter Authentication Key', 'AirStrip ONE', 'Shared Key', 'Site ID', 'User ID', 'Shared Key', 'Email', 'Enable Secure Message Initiation', 'Secure Message Initiation - Incoming Mail', 'Protocol', 'Email Scan Interval (in seconds)', 'Initiation Permitted', and 'Email Username'. At the bottom, there is a 'Description' section and 'OK', 'Cancel', and 'Help' buttons.

Enabled	Yes
Adapter URL	
Adapter Authentication Key	
AirStrip ONE	
Enabled	No
Shared Key	
Site ID	
Vocera Secure Texting App - Message Exchange	
Enabled	Yes
User ID	
Shared Key	
Email	
Enable Secure Message Initiation	No
Secure Message Initiation - Incoming Mail	
Protocol	POP3
Email Scan Interval (in seconds)	30
Initiation Permitted	From VMP users only
Email Username	
Description Setting this to "Yes" enables message and images to be exchanged between users of the Vocera Collaboration Suite and the Vocera Secure Texting mobile applications	

5. In the User ID field, type the ID that the VST cloud server uses to identify the connected Vocera organization.
6. In the Shared Key field, type the key that authenticates the connection between the VST cloud server and the connected Vocera organization.
7. Click OK to save your changes.

8. On the computer on which the VMP Server is running, ensure that outgoing connections on port 443 are not blocked by your firewall. The VMP Server uses this port to transmit information to the VST server.

The **User ID** and **Shared Key** fields are generated from the VST Administration Console. See the *VST Vocera Administrator Guide* for more details.

When the VMP Server synchronizes with the VST cloud server, all VST users on the cloud server are imported into the VMP Server as VMP users. These users also automatically become members of the **VST Users Distribution List**. To control which VMP users can view these VST users as contacts, specify access permissions on this Distribution List. See [Managing Access to a Distribution List](#) on page 160 for more details.

VST Message Routing

Messages sent to merged VST are sent to either the VST client or the badge based on predefined rules.

- Conversation-based messages are delivered to VST clients, not to badges.
- User-generated notifications from the VMP Web Console, VCS, and Staff Assignment are delivered to VST clients, not to badges.
- Third-party system-generated notifications from sources such as VMI, email, WCTP, and CWE are delivered to badges, not to VST clients.

Configuring VMP for Active Directory

You can use the VMP Enterprise Manager to configure VMP to work with an Active Directory server.

The following configuration options are available:

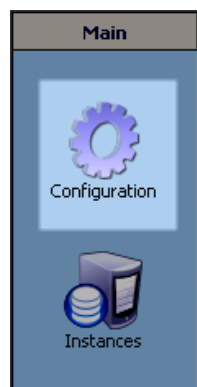
- You can configure the VMP Server to interact with Active Directory using an SSL connection.
- You can allow users to log into the VMP Administrator or VMP Web Console using their Active Directory username and password, provided you have granted permission to these users.

If you specified an Active Directory server when installing VMP, some of the fields described here have already been supplied.



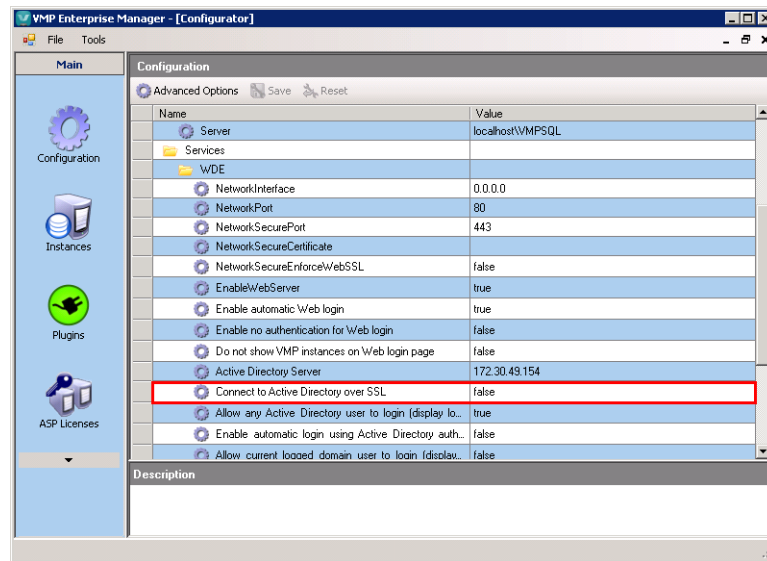
Note: See [Editing User Information](#) on page 122 for more information on how to edit user information to grant user access to the VMP Administrator or the VMP Web Console.

1. Start the VMP Enterprise Manager application:
All Programs > VMP > VMP Enterprise Manager
2. Select Configuration .

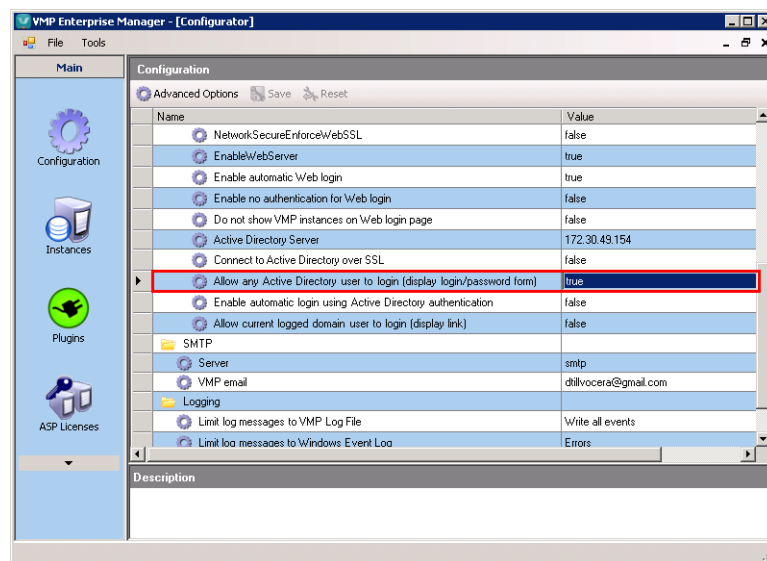


The Configuration window appears.

3. Scroll down to the Active Directory Server field. If this field is empty, type the IP address of the Active Directory server.
4. If you want to use SSL with Active Directory, set the Connect to Active Directory over SSL to true.



5. If you want to enable users to use their Active Directory usernames and passwords to access either the VMP Administrator or the VMP Web Console, depending on granted permissions, set Allow any Active Directory user to login (display login/password form) to true.



6. Save the configuration changes. In the confirmation dialog, click Yes to restart the VMP Server.
7. Click OK to close the restart dialog and complete the configuration.
8. Close the VMP Enterprise Manager.



Note: If you have set up VMP in a clustered environment, you must repeat these instructions for each cluster node on which the VMP Server is installed. To ensure the least amount of down time, integrate the Active Directory on the standby server first, then repeat on the active server.

Engage Integration

You can integrate VMP with an Engage server. This enables users to add information on a patient to a message conversation and view alarms sent by patients or care providers as notifications.

Two types of connections are supported:

- Connections to the Engage Patient Context Adapter, which enable users to add information on a patient to a message conversation.
- Connections from Engage to the VMP SOAP interface, which send alarms sent by patients or care providers as VCS or VMP Web Console notifications.



Note: If you plan to use Engage with VMP, a member of the Vocera Professional Services team will install and configure it for you. Contact your Vocera representative for more details.

To integrate the VMP Server with the Engage environment:

- Ensure that the Active Directory server that your Engage environment is using is also integrated with the VMP Server. This ensures that both the Engage server and the VMP Server use a common user identifier. See [Configuring VMP for Active Directory](#) on page 37 for more information on integrating VMP with Active Directory.
- Specify the following in the VMP Administrator configuration options:
 - The Engage Patient Context Adapter that you are using.
 - If you are displaying waveform information, the AirStrip ONE platform that you are using.
- Create one or more VMP users and grant access rights to the SOAP API gateway. Engage uses this gateway to send alarms as notifications. See [Enabling Engage SOAP Access](#) on page 43 for details on how to enable Engage SOAP access for a VMP user.



Note: If you are upgrading from a previous version of Vocera Voice Server while integrating VMP with Engage, and are therefore replacing a connection between the Engage server and the Vocera Voice Server with a connection between the Engage server and VMP, the Vocera Voice Server VMI license that you have been using for the Engage integration is now freed up.

Integrating with the Engage Patient Context Adapter

You can configure the VMP Server to obtain information from the Engage Patient Context Adapter. This enables Vocera Collaboration Suite and VMP Web Console users to include links to patient information in message conversations.

1. Start the VMP Administrator.
2. Select Configuration > System Options.



The System Options dialog box appears.

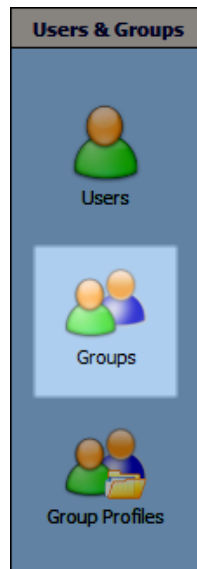
3. Scroll to the Integrations section, and then to the Patient Context subsection.
4. Set the Enabled field to Yes.

System Options	
IP Addresses	172.30.49.161
Port	80
Use HTTPS	No
VCG IP Addresses	
VMI Message Expiry (in minutes)	5
Enable Enhanced Voice Server NIO Tomcat Feature	No
Use VCG for VCS client connection management	No
Patient Context	
Enabled	Yes
Adapter URL	
Adapter Authentication Key	
AirStrip ONE	
Enabled	No
Shared Key	
Site ID	
Vocera Secure Texting App - Message Exchange	
Enabled	No
User ID	
Description	

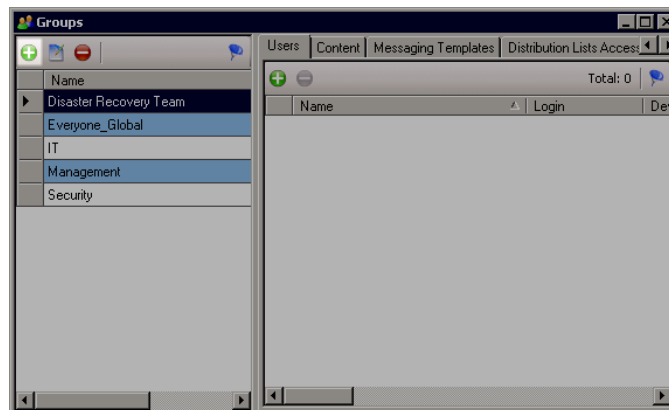
5. In the Adapter URL field, type the URL of the Engage Patient Context Adapter. An example URL is <http://172.30.1.1/myadapter/PatientContext/api/1>.
6. In the Adapter Authentication Key field, type the key that authenticates the connection between the VMP Server and the Engage Patient Context Adapter.
7. Click OK to save your changes.
8. The next step is to create a VMP group containing the users that have permission to access the Engage Patient Context Adapter. To do this, select **Users & Groups > Groups**.



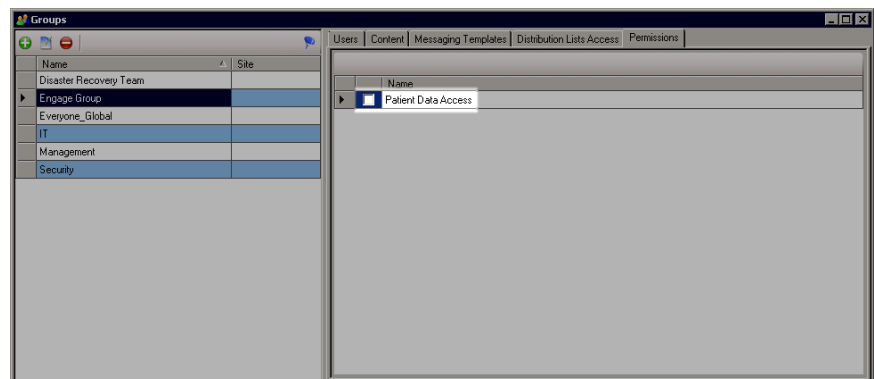
Note: You can also use an existing group, if this fits better with your group organization.



9. If you are creating a new group:
 - a. In the toolbar in the Groups pane, click Add.



- b. In the New Group dialog box, enter the name of the group (for example, **Engage Group**), and click OK.
10. In the Groups view, select the group that is to receive Engage Patient Context Adapter permissions, and click the Permissions tab.
11. Select the Patient Data Access checkbox.



After you have created this group, if you are viewing a user who is a member of the group, and you select the **Member of** tab, the Patient Data Access column indicates that the user is a member of a group that has patient data access.

Member of		
Content Distribution Lists View Sent By - Text Messages View Received By - Text Messages Messaging Templates		
Name	Patient Data Access	Site
Disaster Recovery Team	No	
Engage Group	Yes	
Everyone_Global	No	

The user is also listed as having the Patient Data Access user right:

The 'Edit Rights' dialog box is shown with the 'Rights' tab selected. On the left, under 'Right Groups', 'Custom permissions' is expanded, showing a list of roles including 'Contacts manager', 'Content manager', 'Distribution lists manager', 'Groups manager', 'Own group manager', 'Paging API Gateway', 'Reports viewer', 'Superuser', 'System manager', and 'Users manager'. On the right, under 'Rights', a list of permissions is shown, including 'Manage contact distribution lists', 'Manage contact sources', 'Manage distribution lists', 'Manage groups user belongs to', 'Manage schedules', 'Manage who views VMP text messages', 'View all distribution lists', 'View all messaging templates', 'View all pager alerts in the report', 'View all reports', and 'Patient Data Access'. The 'Patient Data Access' checkbox is checked. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

This user right is not editable in the Edit Rights dialog box.



Note:

If you want Vocera Collaboration Suite users to be able to access AirStrip ONE waveforms when displaying patient information obtained from the Engage Patient Context Adapter, you must integrate the VMP Server with an AirStrip ONE platform. See [Integrating with the AirStrip ONE Platform](#) on page 42 for more details.

Integrating with the AirStrip ONE Platform

You can configure the VMP Server to integrate with an AirStrip ONE platform. This enables Vocera Collaboration Suite users to display waveform data when viewing patient information obtained from the Engage Patient Context Adapter.

1. Start the VMP Administrator.
2. Select Configuration > System Options.



The System Options dialog box appears.

3. Scroll to the Integrations section, and then to the AirStrip ONE subsection.
4. Set the Enabled field to Yes.

System Options	
IP Addresses	172.30.49.161
Port	80
Use HTTPS	No
VCG IP Addresses	
VMI Message Expiry (in minutes)	5
Enable Enhanced Voice Server NIO Tomcat Feature	No
Use VCG for VCS client connection management	No
Patient Context	
Enabled	Yes
Adapter URL	
Adapter Authentication Key	
AirStrip ONE	
Enabled	Yes
Shared Key	
Site ID	
Vocera Secure Texting App - Message Exchange	
Enabled	No
User ID	
Description	
Whether or not AirStrip ONE integration is available	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

5. In the Shared Key field, type the AirStrip ONE authentication key.
6. In the Site ID field, type the AirStrip ONE site ID.
7. Click OK to save your changes.

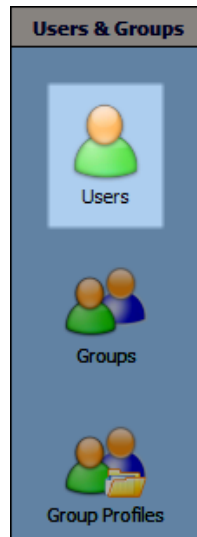
Enabling Engage SOAP Access

You can create a VMP user and enable SOAP access for this user from Engage.

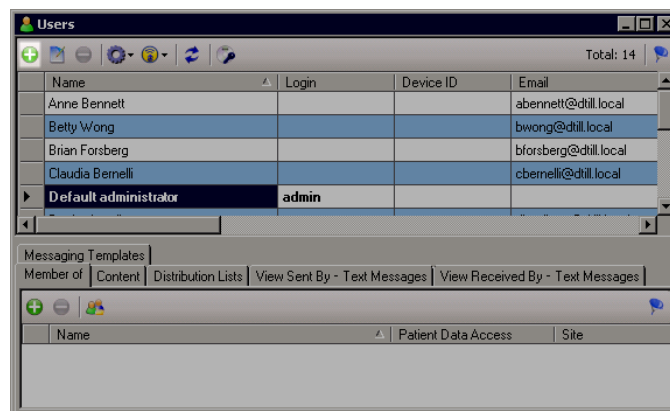


Note: To enable SOAP access from Engage, VMP must be licensed to use the Pager Inbound SOAP Connector. By default, VMP licenses do not include this connector. See [Configuring the VMP License](#) on page 19 for more information on licensing.

1. From the VMP Administrator, select Users & Groups > Users.



2. In the toolbar in the Users pane, click Add.



The End-User Settings window appears.

3. Enter the following end-user settings.

Table 17: End-user settings

Field	Description
First Name	The first name of the user.
Middle Name	The middle name of the user (optional).
Last Name	The last name of the user.
Title	The job title for the user.
Email	The email address for the user.
Enable PC Admin Console Access	Select this checkbox to allow the user to access the VMP Administrator.
Vocera credentials	Provide Vocera credentials for the new user: enter the VMP Administrator login in the Login field, enter the password in the Password field, and re-enter the password in the Confirmation field.

4. Click Next to display the Push Technology and Licensing window. Ensure that the Enable checkbox in the Mobile Device Access section is cleared.

Edit User

Step 2: Push Technology and Licensing

Step 1: End-User Settings
Step 2: Push Technology and Licensing

Mobile Device Access

☐ Enable

Device type: Vocera Smartphone Client

Registration Key: ☐ Generate key

Device PIN:

Enforce App PIN: Follow System Settings (Shared)

VMP Applications On Device

	Application Name
<input checked="" type="checkbox"/>	Alert
<input type="checkbox"/>	Alert(SMS)
<input type="checkbox"/>	Alert(SNPP/WCTP/TAP)
<input type="checkbox"/>	Chat
<input type="checkbox"/>	Contacts
<input type="checkbox"/>	Content

< Back Finish Cancel Help

5. Click Finish to create the user.
6. In the Users view, select the user that you have just created.
7. In the toolbar, from the User preferences dropdown list, select User rights.

Users

Total: 14

Name	Device ID	Email
Anne Bennett		abennett@dhill.local
Betty Wong		bwong@dhill.local
Brian Forsberg		bforsberg@dhill.local
Claudia Bernelli		cbernelli@dhill.local

Default administrator: admin

Messaging Templates

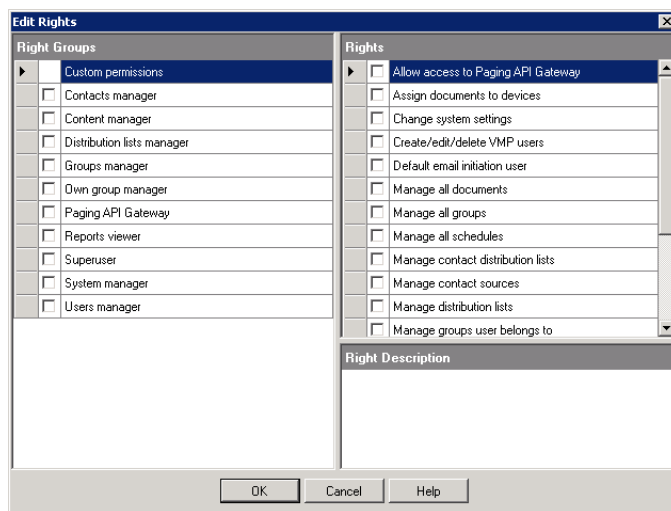
Member of: Content Distribution Lists View Sent By - Text Messages View Received By - Text Messages

User preferences dropdown menu:

- User rights
- Unlock user
- Applications on device
- Plugins configuration
- Retrieve Application Logs

Name	Patient Data Access	Site
Everyone_Global	No	

The Edit Rights dialog box appears.



8. In the Rights pane, select Allow access to Paging API Gateway.
9. Click OK.

About Importing and Synchronizing

Use the VMP Administrator to import users and contacts into the VMP Server from one or more sources.

If a user with the same email address, Public ID, Pager ID or Vocera ID is imported from multiple sources, the VMP Server merges the information from these sources into a single VMP user entry.



Note: A user and a contact are linked if the email address is the same for both.

You can import from any or all of the following sources:

- Vocera Voice Server: see [Importing Users From Vocera Voice Server](#) on page 49
- Active Directory: see [Importing Users From Active Directory](#) on page 51
- Excel and CSV files: see [Importing Users From an Excel or CSV File](#) on page 54
- SQL: see [Importing Users From SQL](#) on page 56

You can synchronize the VMP Server with its sources to ensure that the list of users and contacts is kept up to date. You can start the synchronization process manually, or configure the VMP Server to synchronize at regular intervals.

Vocera Secure Texting users are automatically imported when VST message exchange is enabled. See [Enabling VST Message Exchange](#) on page 35 for more details.

Attention: Each user or contact on the VMP Server must have a unique email address, Public ID, Pager ID, or Vocera ID, as these fields are used as key fields. If multiple users or contacts have the same email address, Public ID, Pager ID, or Vocera ID, the VMP Server may not operate as expected.



Tip: You can customize the field mappings that the VMP Server will use when importing users or contacts. For details about source field mapping, see [About User Field Editing](#) on page 187 and [About Contact Fields](#) on page 185.



Note: BlackBerry Enterprise Server (BES) sources are included in the list of available source types, but are no longer supported.

About Users and Contacts

When importing from sources into the VMP Server, you can import both users and contacts.

A user is anyone who can send or receive a message from a licensed device, from the VMP Web Console, or by email. Most users are employees who have application licenses assigned to them. Some users who generate messages but do not receive them do not need application licenses.

Contacts are parties who may or may not be part of your organization, but with whom critical and frequent communication occurs. You can think of contacts as a set of employees and non-employees who are entered into the system with one or many contact points for easy communication.

Importing Users From Vocera Voice Server

If you plan to integrate the VMP Server with a Vocera Voice Server, you must import the Vocera Voice Server users into the VMP Server.



Note: See [Vocera Voice Server Integration](#) on page 30 for information on integrating the VMP Server with a Vocera Voice Server.

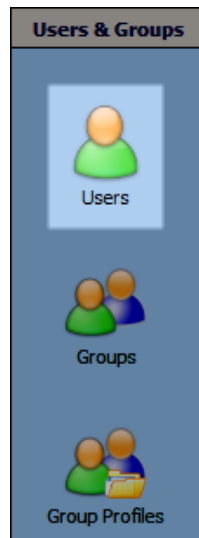


Important: If you are using the email address field to match Vocera Voice Server users with VMP users, ensure that each Vocera Voice Server user has an email address defined. This prevents duplicate user entries. This does not apply if you are matching Vocera Voice Server user IDs to Active Directory fields.

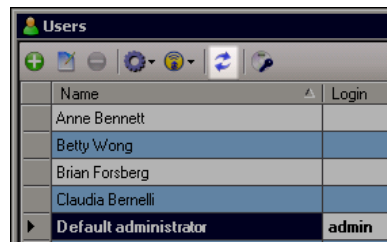


Note: If a Vocera Voice Server user has been linked to a Vocera Secure Texting account, this user cannot access the Vocera Collaboration Suite.

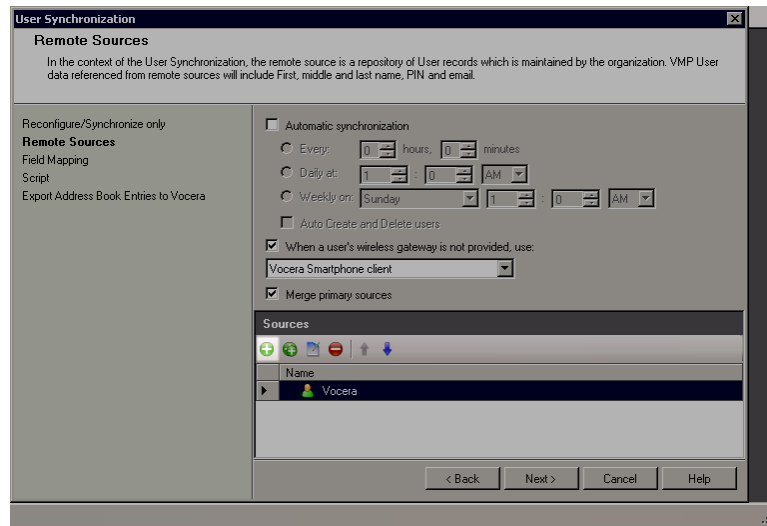
1. Select Users & Groups > Users.



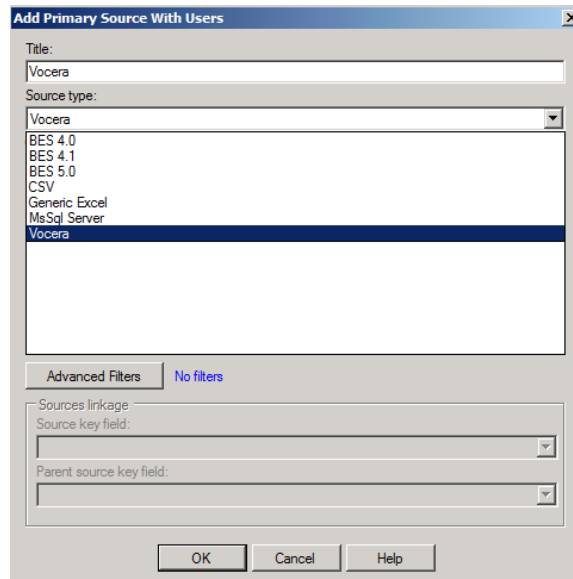
2. Click Synchronization in the Users view.



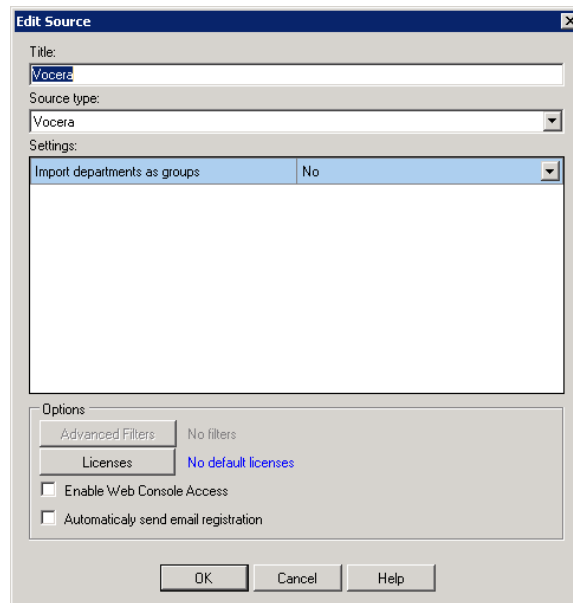
3. If you have previously imported one or more sources into the VMP Server, the Reconfigure/Synchronize only window appears. Select Yes, reconfigure settings and click Next.
4. In the User Synchronization dialog, click Add primary source with users (under Sources).



5. Select Vocera from the Source type dropdown list. This selection auto-populates the Title field. You can accept the default title or customize the title.



6. Set Import departments as groups to Yes if you want to import Vocera Voice Server departments into the VMP Server as VMP groups.



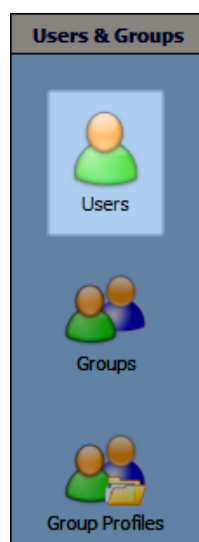
Note: The availability of this feature depends on the Vocera Voice Server version that you have installed.

7. Optionally specify the import source options described in [Specifying Source Importing Options](#) on page 58.
8. Click OK to close the dialog.
9. Follow the steps in [Synchronizing Users and Contacts](#) on page 60 to synchronize the Vocera Voice Server users and contacts with the VMP Server.

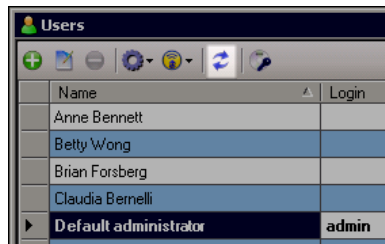
Importing Users From Active Directory

The VMP Server can synchronize with an Active Directory server to import Organizational Units, security groups, and Distribution Lists. When an import is complete, VMP has the ability to convert the Organizational Units to VMP Distribution Lists.

1. Select Users & Groups > Users.

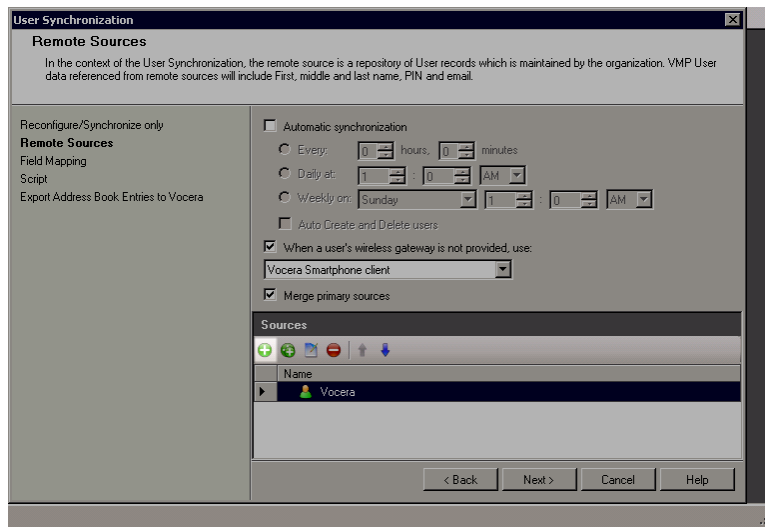


2. Click Synchronization in the Users view.



Name	Login
Anne Bennett	
Betty Wong	
Brian Forsberg	
Claudia Bernelli	
Default administrator	admin

3. If you have previously imported one or more sources into the VMP Server, the Reconfigure/Synchronize only window appears. Select Yes, reconfigure settings and click Next.
4. In the User Synchronization dialog, click Add primary source with users (under Sources).



User Synchronization

Remote Sources
In the context of the User Synchronization, the remote source is a repository of User records which is maintained by the organization. VMP User data referenced from remote sources will include First, middle and last name, PIN and email.

Reconfigure/Synchronize only
Remote Sources
Field Mapping
Script
Export Address Book Entries to Vocera

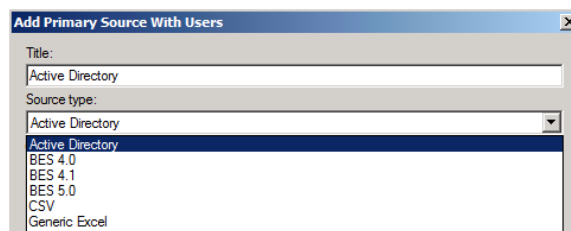
☐ Automatic synchronization
☐ Every: 0 hours, 0 minutes
☐ Daily at: 1 : 0 AM
☐ Weekly on: Sunday 1 : 0 AM
☐ Auto Create and Delete users
☒ When a user's wireless gateway is not provided, use:
Vocera Smartphone client
☒ Merge primary sources

Sources

Name
Vocera

< Back Next > Cancel Help

5. Select Active Directory from the Source type dropdown list. This selection auto-populates the Title field. You can accept the default title or customize the title.



Add Primary Source With Users

Title: Active Directory

Source type: Active Directory

Active Directory
BES 4.0
BES 4.1
BES 5.0
CSV
Generic Excel
LDAP

6. In the Connection Parameters section, enter the Active Directory credentials.

Edit Source

Title:

Source type:

Settings:

Host	172.30.49.151
Port	389
Connect over SSL	No
Username	sa
Password	*****
Confirm Password	*****
Sync Organizational Units	No
Sync Security Groups	Yes
Sync Distribution Groups	No

Options:

[No filters](#)

[No default licenses](#)

☐ Enable Web Console Access

☐ Automatically send email registration

7. Configure the following options using their associated dropdown lists:
 - Sync Organization Units
 - Sync Security Groups
 - Sync Distribution Groups
8. Optionally specify the import source options described in [Specifying Source Importing Options](#) on page 58.
9. Click **OK** to close the dialog.
10. Follow the steps in [Synchronizing Users and Contacts](#) on page 60 to synchronize the Vocera Voice Server users and contacts with the VMP Server.

Displaying Active Directory Profile Pictures in VCS

If your Active Directory server includes user photographs in the `thumbnailPhoto` source field, you can ensure that these photographs are displayed in the Vocera Collaboration Suite.

1. Create a contact source for the Active Directory server. See [Importing Contacts From a Source](#) on page 67 for details on how to do this.
2. In this contact source, map the `Personal Photo` contact field to `thumbnailPhoto`, and set the `Key` and `User Key` checkboxes in the row that contains the `Email` contact field.

Edit Contact Source

Field Mapping

Contact Synchronization is an automated procedure defined by the VMP Administrator whereby all contact records stored on all remote sources that the VMP system is referencing are checked for changes, and any new or changed Contact information is detected and pushed out to the appropriate VMP-enabled devices.

Reconfigure/Synchronize only
Contact Source Name
Remote Sources
Select Contacts
Contact/DL Synchronization
Field Mapping

Sources

Name
Active Directory

Fields Mapping

Contact field	Source	Source field	Key	User Key
Personal Photo	Active Direct...	thumbnailPhoto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
First Name	Active Direct...	First name	<input type="checkbox"/>	<input type="checkbox"/>
Middle Name			<input type="checkbox"/>	<input type="checkbox"/>
Last Name	Active Direct...	Last name	<input type="checkbox"/>	<input type="checkbox"/>
BlackBerry PIN			<input type="checkbox"/>	<input type="checkbox"/>
Email	Active Direct...	E-mail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Photo			<input type="checkbox"/>	<input type="checkbox"/>
Image 1			<input type="checkbox"/>	<input type="checkbox"/>

< Back Finish Cancel Help

3. Create a Contacts Distribution List for the Active Directory users for which photos are to be displayed. See [Creating a Contacts Distribution List](#) on page 139 for more details.

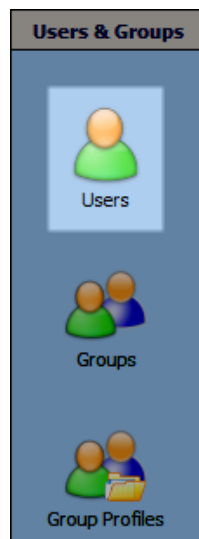
Importing Users From an Excel or CSV File

If your list of users is stored in an Excel spreadsheet or CSV file, you can import these users into the VMP Administrator.



Tip: Avoid using an Excel or CSV file as a user or contact source if at all possible, as difficulties may arise if this file becomes no longer available.

1. Select Users & Groups > Users.

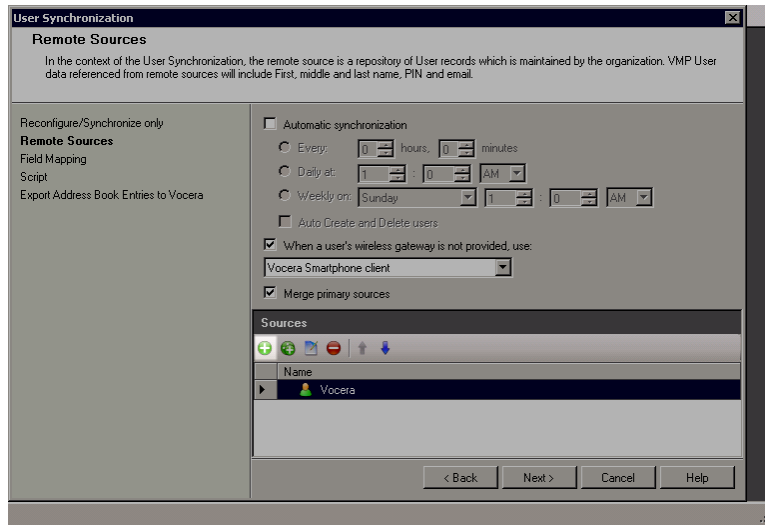


2. Click Synchronization in the Users view.



Name	Login
Anne Bennett	
Betty Wong	
Brian Forsberg	
Claudia Bernelli	
Default administrator	admin

- If you have previously imported one or more sources into the VMP Server, the Reconfigure/Synchronize only window appears. Select Yes, reconfigure settings and click Next.
- In the User Synchronization dialog, click Add primary source with users (under Sources).



User Synchronization

Remote Sources
In the context of the User Synchronization, the remote source is a repository of User records which is maintained by the organization. VMP User data referenced from remote sources will include First, middle and last name, PIN and email.

Reconfigure/Synchronize only
Remote Sources
Field Mapping
Script
Export Address Book Entries to Vocera

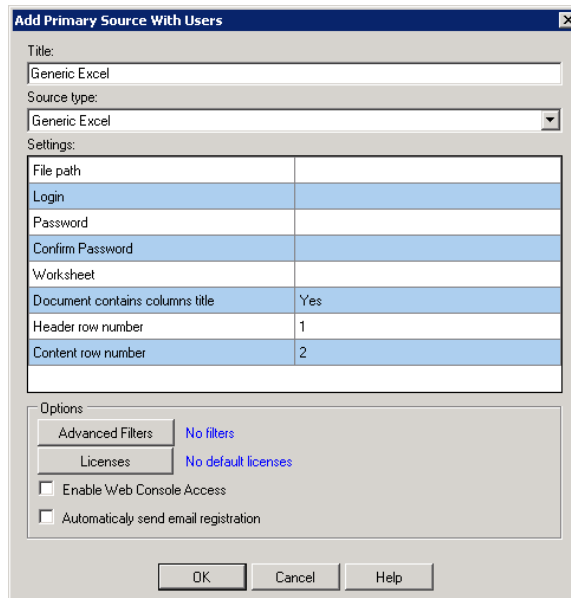
☐ Automatic synchronization
☐ Every: 0 hours, 0 minutes
☐ Daily at: 1 : 0 AM
☐ Weekly on: Sunday 1 : 0 AM
☐ Auto Create and Delete users
☒ When a user's wireless gateway is not provided, use:
Vocera Smartphone client
☒ Merge primary sources

Sources

Name
Vocera

< Back Next > Cancel Help

- Select Generic Excel or CSV from the Source type dropdown list. This selection auto-populates the Title field. You can accept the default title or customize the title.
- If your file is an Excel file, edit the connection parameters listed below.



Add Primary Source With Users

Title: Generic Excel

Source type: Generic Excel

Settings:

File path	
Login	
Password	
Confirm Password	
Worksheet	
Document contains columns title	Yes
Header row number	1
Content row number	2

Options:

Advanced Filters: No filters
Licenses: No default licenses

☐ Enable Web Console Access
☐ Automatically send email registration

OK Cancel Help


Table 18: Generic Excel connection parameters

Parameter	Description
File path	Click in this field to browse for the file, or type the path in the box.
Login	If required, enter a login and a password to access the Excel file.

Parameter	Description
Password	
Confirm Password	If a login and password are required to access the file, enter the password a second time to confirm the credentials.
Worksheet	If the spreadsheet includes more than one worksheet, enter the name of the worksheet to import as source data.
Document contains columns title	Select Yes if the spreadsheet uses title columns to define the data. Select No if the spreadsheet does not include title columns.
Header row number	Enter the header row number.
Content row number	Enter the content row number.

- If your file is a CSV file, edit the connection parameters listed below.

Table 19: CSV connection parameters

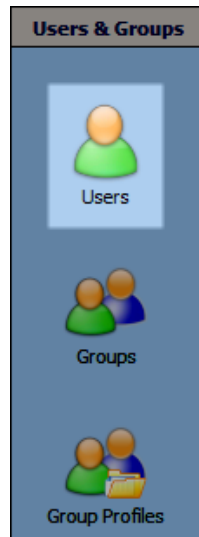
Parameter	Description
File path	Click in this field to browse for the file, or type the path in the box.  Note: If your file resides on a remote network, automatic synchronization will not work unless the Vocera Data Exchange service is modified to use the local administrator account instead of the VMP local system account.
Login	If required, enter a login and a password to access the CSV file.
Password	
Confirm Password	If a login and password are required to access the file, enter the password a second time to confirm the credentials.
Encoding	Select the text encoding option appropriate for the imported data. In most cases, the default option of <i>Automatic</i> is appropriate.
Delimiter	Use the dropdown list to choose a comma or semicolon as the string separator.
Document contains columns title	Select Yes if the spreadsheet uses title columns to define the data. Select No if the spreadsheet does not include title columns.

- Optionally specify the import source options described in [Specifying Source Importing Options](#) on page 58.
- Click OK to close the dialog.
- Follow the steps in [Synchronizing Users and Contacts](#) on page 60 to synchronize the Excel or CSV file users and contacts with the VMP Server.

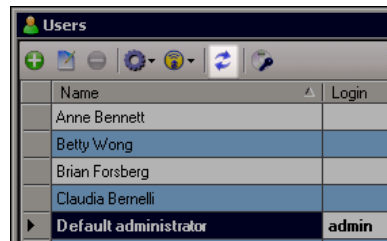
Importing Users From SQL

If you have your own SQL database for keeping track of user information, you can import the users from this database into the VMP Server.

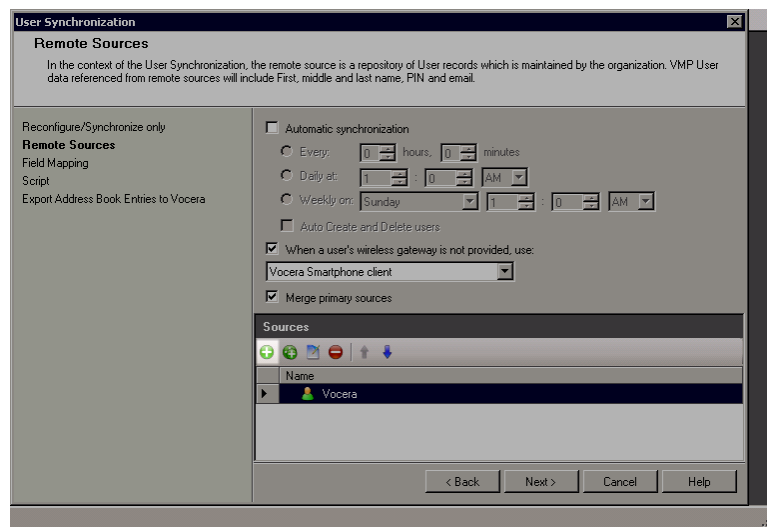
- Select **Users & Groups > Users**.



2. Click Synchronization in the Users view.



3. If you have previously imported one or more sources into the VMP Server, the Reconfigure/Synchronize only window appears. Select Yes, reconfigure settings and click Next.
4. In the User Synchronization dialog, click Add primary source with users (under Sources).



5. Select MsSqlServer from the Source type dropdown list. This selection auto-populates the Title field. You can accept the default title or customize the title.
6. Enter the Connection Parameters.

Table 20: SQL connection parameters

Parameter	Description
Address	The computer name or IP address of the SQL server.
Login	The SA login credentials.
Password	
Confirm Password	Enter the password a second time to confirm the credentials.
Database	Select the database to import from the dropdown list.
Query	Use the dropdown list to select any specific query options for the import.

- Optionally specify the import source options described in [Specifying Source Importing Options](#) on page 58.
- Click OK to close the dialog.
- Follow the steps in [Synchronizing Users and Contacts](#) on page 60 to synchronize the SQL users and contacts with the VMP Server.

Specifying Source Importing Options

When you are importing users from a source, you can use the source importing options to specify which users to import, enable VMP Web Console access, assign licenses, or email registration instructions.

Edit Source

Title: Active Directory

Source type: Active Directory

Settings:

Host	172.30.49.151
Port	389
Connect over SSL	No
Username	sa
Password	XXXXXXXXXX
Confirm Password	XXXXXXXXXX
Sync Organizational Units	No
Sync Security Groups	Yes
Sync Distribution Groups	No

Options

Advanced Filters No filters

Licenses No default licenses

☐ Enable Web Console Access

☐ Automatically send email registration

OK Cancel Help

To specify source importing options:

1. If the Advanced Filters button is enabled, click it to display the advanced filtering options for this import source operation. These filters enable you to specify which users are to be imported from the source.

Advanced Filters

Contact types

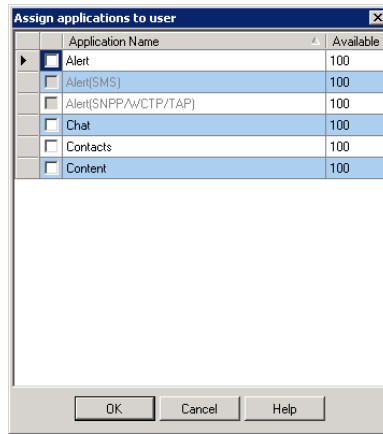
☒ Users ☒ Contacts ☒ InetOrgPersons

☒ Enable fields filtration

accountExpires Contains

OK Cancel Help

2. In the Contact types pane, select the check boxes of the types of users that you want to import.
3. Select Enable fields filtration to specify that only users that match the specified criteria are to be imported. In the list of fields displayed, select the filtration criteria that you want to use.
4. Click OK to close the Advanced Filters dialog box.
5. Click Licenses to display the Assign applications to user dialog box.



6. In this dialog box, specify the application licenses that are to be granted by default to all imported users.
7. Click **OK** to close this dialog box.
8. Select the **Enable Web Console Access** check box if imported users are to be granted VMP Web Console access by default.
9. Select the **Automatically send email registration** check box to automatically email registration instructions to all imported users.

Synchronizing Users and Contacts

After you have specified the sources for the VMP Server, you can synchronize your sources with the server to ensure that all information is up to date. You can synchronize manually or set up automatic synchronization.

The following synchronizations happen automatically, whether or not you have set up automatic synchronization:

- If a Vocera Voice Server has been set up as a source, the VMP Server is automatically updated whenever a Vocera Voice Server user is added, edited, or deleted.
- If the VMP Server has been integrated with Vocera Secure Texting, the VMP Server is automatically updated whenever a VST user is added, edited, or merged with a Vocera Voice Server user. When a VST user is deleted, the VMP Server is updated within 10 minutes.



Note: Contacts are never automatically synchronized.

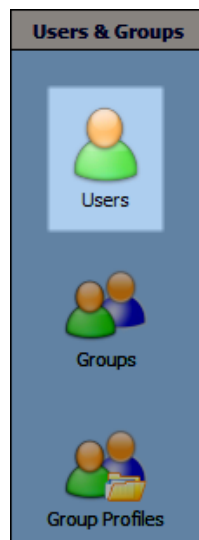
The steps of the synchronization process depend on the sources that you have specified. The following screens are included:

Screen	Description
Reconfigure/Synchronize only	Specifies whether to reconfigure import sources before synchronization. This screen appears if you have already imported at least one source.
Remote Sources	Lists the remote sources to be used in synchronization. Also enables you to specify automatic synchronization.
Select Users	If you are importing from an Active Directory source, this screen enables you to specify which Organizational Units (OUs) are to be synchronized to create a VMP Distribution List.
User/DL Synchronization	If you are importing from an Active Directory source, this screen enables you to specify whether to import users only, or whether to also import the OU hierarchy. If you are importing the OU hierarchy, you can specify whether you want the VMP Server to automatically create Distribution Lists from the imported OUs.

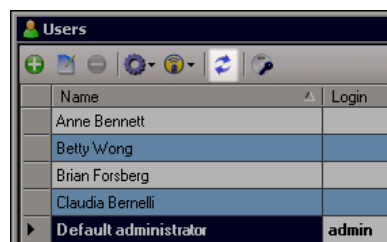
Screen	Description
Default DL Permissions	This screen appears only if you are importing from an Active Directory source and you are importing the OU hierarchy. For the initial Active Directory import, you can configure permissions for the default administrator and any groups selected for import.
Field Mapping	For each selected source, this screen specifies how fields in the source are to be mapped to VMP user fields.
Script	Creates the internal script that performs the synchronization. In this screen, you can manually specify the users or contacts to be added or updated and configure contact options before running the script. These options can be changed manually at any time after deployment. This screen is useful for defining device and wireless gateway assignments.
Export Address Book Entries to Vocera	If you are importing from a Vocera Voice Server, this screen enables you to export a CSV file containing a list of the VMP users that do not have a Vocera ID. You can use this file to create address book entries in the Vocera Voice Server. See Address Book Entry Exporting on page 35 for more information on this capability.

Follow the steps shown below to perform a synchronization.

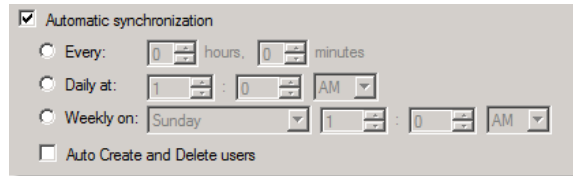
1. In the VMP Administrator, select **Users & Groups > Users**.



2. Click **Synchronization** in the **Users** view.

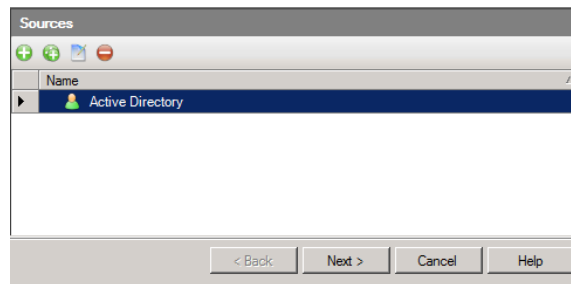


3. If the **Reconfigure/Synchronize only** screen appears, select **Yes**, reconfigure settings.
4. Click **Next**.
5. In the **Remote Sources** screen, you can enable automatic synchronization of user data from the selected sources:
 - a. Select the **Automatic synchronization** checkbox.
 - b. Select one of the following:
 - **Every:** Synchronize after the specified number of hours and minutes has elapsed.
 - **Daily at:** Synchronize every day at the specified time.
 - **Weekly on:** Synchronize once a week at the specified day and time.



Tip: The best auto synchronization time depends on your specific environment. The setting should keep the system updated with new and updated user data and occur when network traffic is not typically heavy.

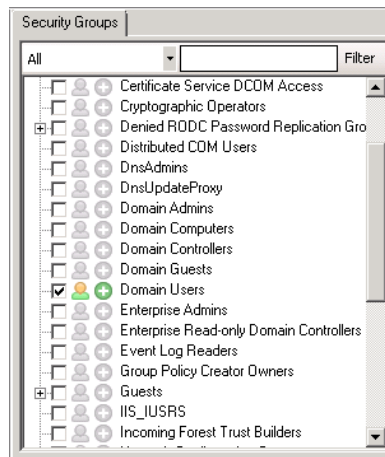
- c. Select Auto Create and Delete users if users that have been added or deleted in the source are to be automatically added or deleted in the VMP Administrator.
6. Clear the When a user's wireless gateway is not provided, use checkbox.
7. Ensure that the Merge primary sources checkbox is selected.
8. Click Next.



9. The Select Users screen appears if you have included Active Directory as a source. In this screen, select the Active Directory users to import by clicking the checkbox next to the Organization Unit (OU) name, if you have not already done this.

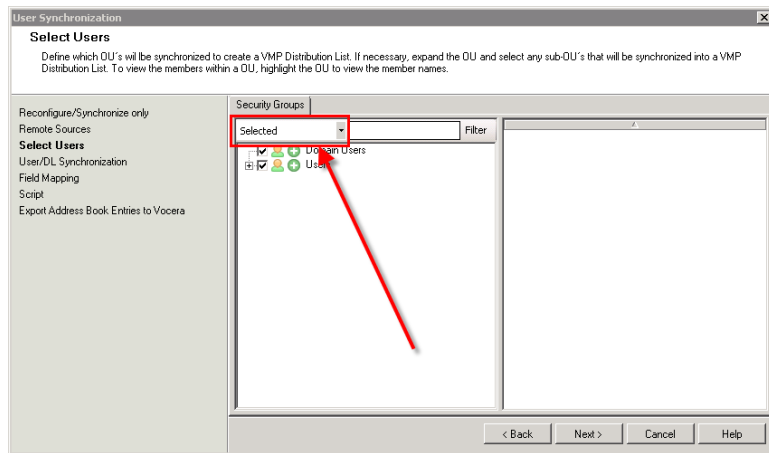
Depending on the user import configuration, the options may be included in the following three tabs:

- Organization Units
 - Security Groups
 - Distribution Groups
- a. To import an OU, select its checkbox.

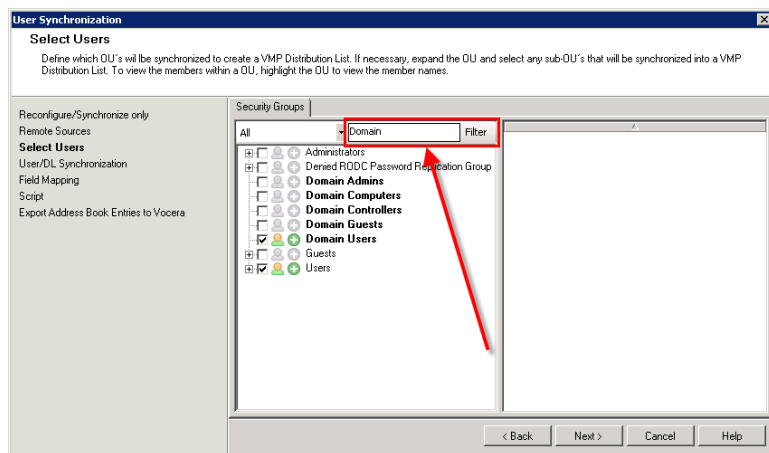


To import a sub-OU, expand the OU and select its checkbox.

- b. To limit the display of OUs, use either or both of the following:
 - From the dropdown list, select Selected to display only the OUs that you have selected.

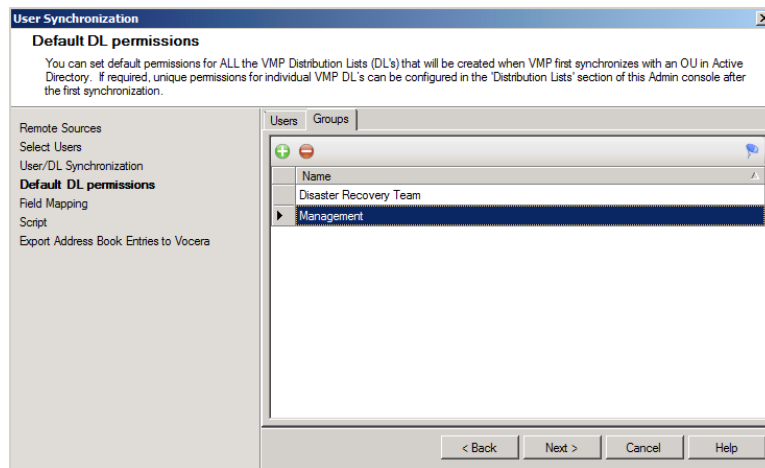


- To filter the OU list, type text in the field provided and click **Filter**. Only the OUs that contain the filter text are displayed, along with some OUs that are always displayed.



To remove the filter, clear the text field and click **Filter** again.

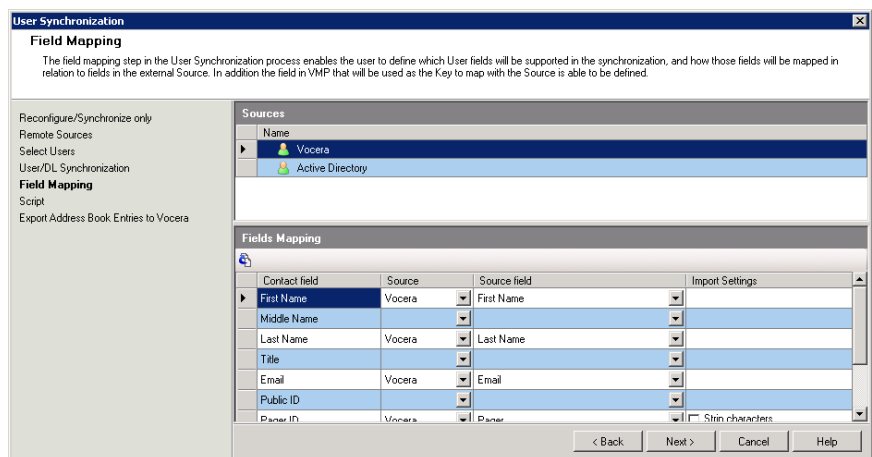
- c. Click **Next**.
10. The **User/DL Synchronization** screen appears if you have included Active Directory as a source. In this screen, use the radio button selection to configure the Active Directory synchronization options appropriate for your deployment. Depending on the user import configuration, the options are included in the following three tabs:
 - Organization Units
 - Security Groups
 - Distribution Groups
 - a. Click each tab to configure the options for the group.
You can import only the users or import the existing OU hierarchy.
 - b. When the options are selected, click **Next**.
11. The **Default DL Permissions** screen appears if you have included Active Directory as a source and are importing the existing OU hierarchy. In this screen, configure permissions for the default administrator and any groups selected for import. Use the tabs to toggle between User and Group permissions. When the configuration is complete, click **Next**.



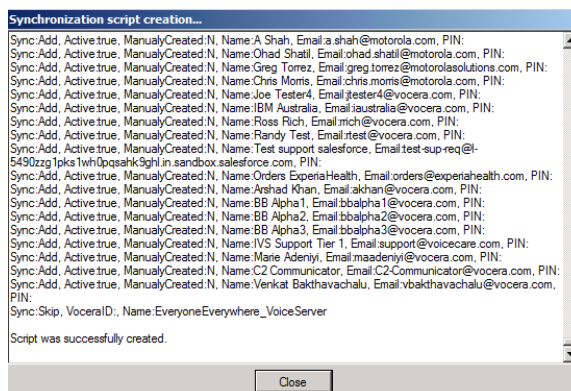
12. In the Field Mapping window, define the field mappings for your deployment, and click Next. By default, the VMP Server uses email addresses to synchronize contacts between sources. If your environment does not use email addresses, you can synchronize between the Vocera Voice Server User ID field and the a field in your Active Directory server (such as sAMAccountName). See [Synchronizing Using Vocera UserID and Active Directory](#) on page 66 for details on how to do this.



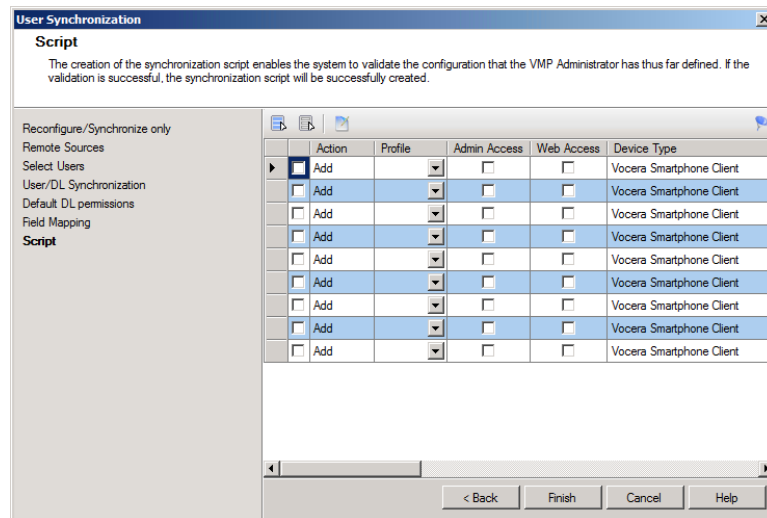
Note: For more information about field mappings, see [About Contact Fields](#) on page 185 and [About Contact Fields](#) on page 186.



13. The synchronization script is generated by the import wizard options selected and is revealed in a script dialog box. Use the scroll bar to review the script and click Close.



14. In the Script dialog, configure the script options as needed:



User Synchronization

Script

The creation of the synchronization script enables the system to validate the configuration that the VMP Administrator has thus far defined. If the validation is successful, the synchronization script will be successfully created.

Reconfigure/Synchronize only

Remote Sources

Select Users

User/DL Synchronization

Default DL permissions

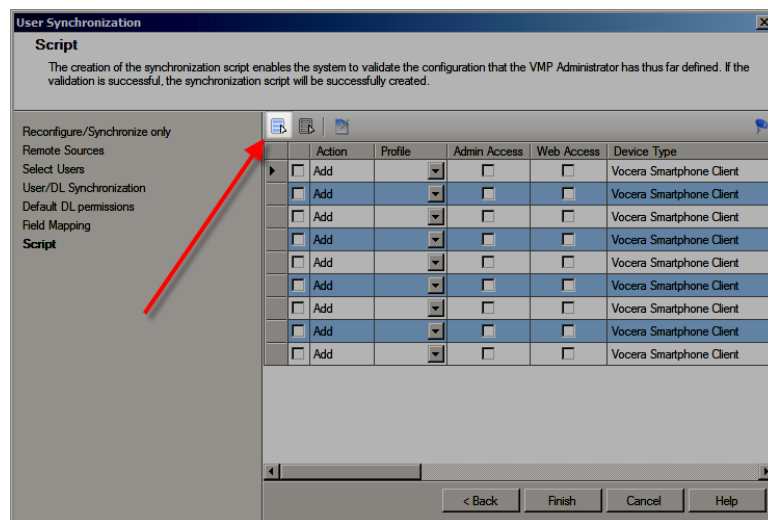
Field Mapping

Script

Action	Profile	Admin Access	Web Access	Device Type
<input checked="" type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client

< Back Finish Cancel Help

- a. Click Check All to confirm the previously configured values.



User Synchronization

Script

The creation of the synchronization script enables the system to validate the configuration that the VMP Administrator has thus far defined. If the validation is successful, the synchronization script will be successfully created.

Reconfigure/Synchronize only

Remote Sources

Select Users

User/DL Synchronization

Default DL permissions

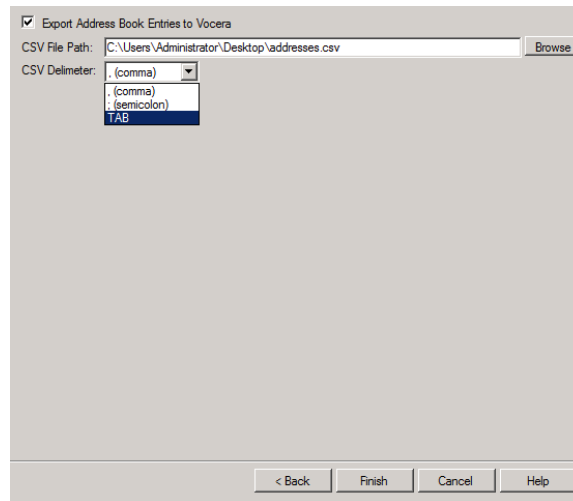
Field Mapping

Script

Action	Profile	Admin Access	Web Access	Device Type
<input checked="" type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client
<input type="checkbox"/> Add		<input type="checkbox"/>	<input type="checkbox"/>	Vocera Smartphone Client

< Back Finish Cancel Help

- b. To specify that a user imported using this script is to be given access to the VMP Administrator, select the **Admin Access** checkbox.
- c. To specify that a user imported using this script is to be given access to the VMP Web Console, select the **Web Access** checkbox.
- d. When you have finished configuration, click **Next** or **Finish** to continue. (The button that appears here depends on whether the **Export Address Book Entries to Vocera** screen appears.)
15. The **Export Address Book Entries to Vocera** screen appears if you have included the Vocera Voice Server as a source. In this screen, select the **Export Address Book Entries to Vocera** checkbox to export a CSV file containing a list of the VMP users that do not have a Vocera ID. You can use this file to create address book entries in the Vocera Voice Server. See [Address Book Entry Exporting](#) on page 35 for more information on this capability.



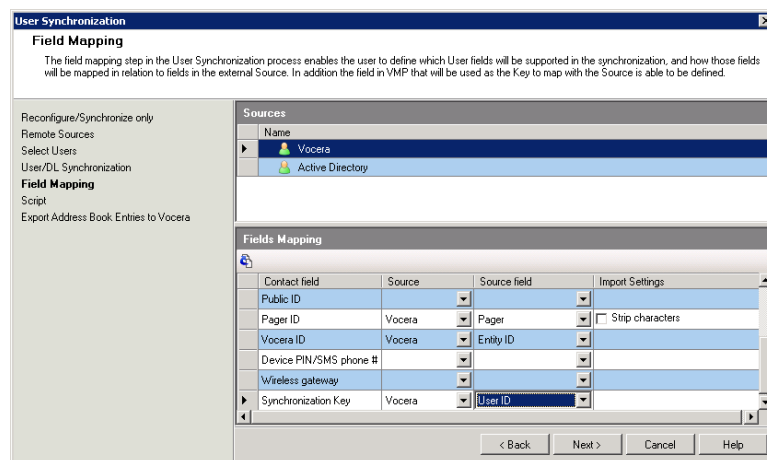
Click Finish to continue.

16. The synchronization script runs. When the sync is complete, click OK to close the successful sync dialog, and click Close to close the script window.

Synchronizing Using Vocera UserID and Active Directory

By default, the VMP Server synchronizes using the email address of each user defined in each source. If you have imported the Vocera and Active Directory sources, you can now synchronize the User ID field in the Vocera source with the a field in the Active Directory source, such as the sAMAccountName field. This is useful in environments where users do not have email addresses.

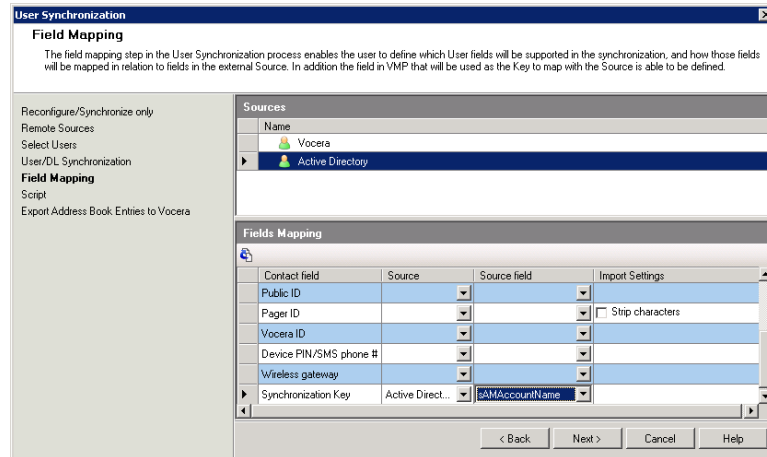
1. Follow the steps described in [Synchronizing Users and Contacts](#) on page 60 to start the synchronization process.
2. When you reach the Field Mapping screen, select the Vocera source.
3. Scroll down to the Synchronization Key row.
4. In the Source column of the Synchronization Key row, select Vocera.
5. In the Source field column of the Synchronization Key row, select User ID.



Note: By default, in the Vocera ID row, the Source field column is set to Entity ID. Do not change this.

6. Select the Active Directory source.
7. Scroll down to the Synchronization Key row.
8. In the Source column of the Synchronization Key row, select Active Directory.

9. In the **Source** field column of the **Synchronization Key** row, select the field that you want to use to synchronize (such as `sAMAccountName`).



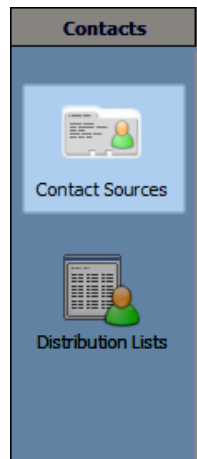
10. Click **Next** to complete the field mapping.
11. Continue following the instructions in [Synchronizing Users and Contacts](#) on page 60 to finish user synchronization.

Importing Contacts From a Source

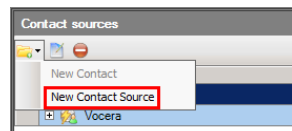
If you have an external source of contact information, you can import the contacts into the VMP Server. You can then regularly synchronize the external source with the VMP Server.

For information on how to import contacts from a Vocera Voice Server global address book, see [Importing Contacts From a Vocera Voice Server Address Book](#) on page 68.

1. Select the **Contacts** module, and select **Contact Sources**.

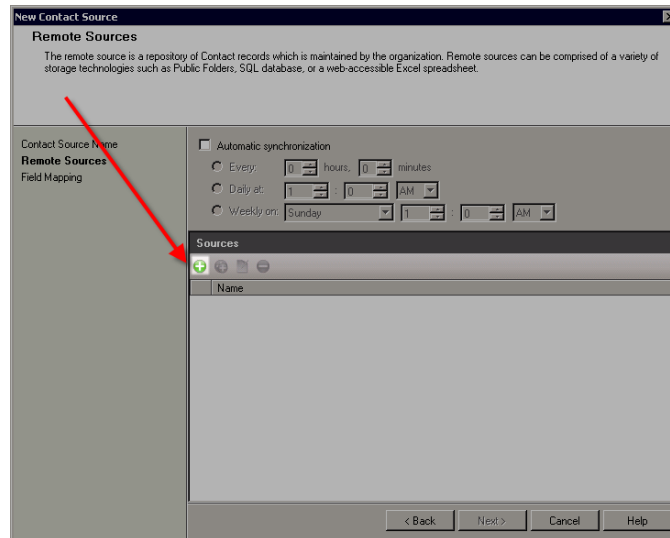


2. Select **New** and choose **New Contact Source**.

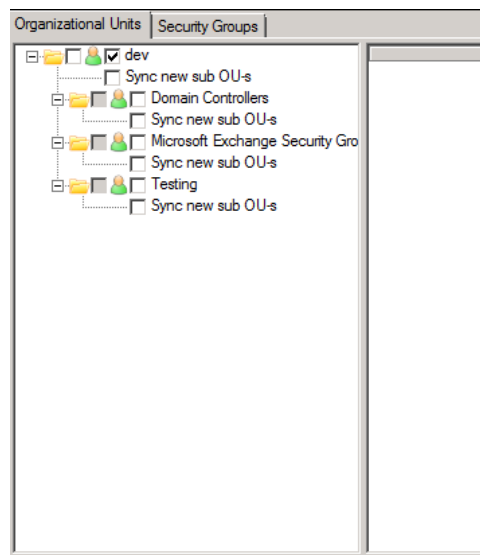


3. Enter a name for the new source, select the **Associated with remote source** checkbox, and click **Next**.
4. If you want the VMP Server to be synchronized with this source:
 - a. Select the **Automatic synchronization** checkbox.
 - b. Select whether you want to synchronize every few hours, daily, or weekly, and then select the time period or time at which synchronization is to take place.

5. Select an existing source or click Add primary source with contacts.



6. If the import is from Active Directory, select the contacts and groups to import, and click Next.



7. If the import is from Active Directory, configure group and Distribution List import options, and click Next.
8. Customize the Field Mappings, if desired, and click Finish.



Note: For more information about field mappings, see [About Contact Fields](#) on page 185 and [About User Field Editing](#) on page 187.

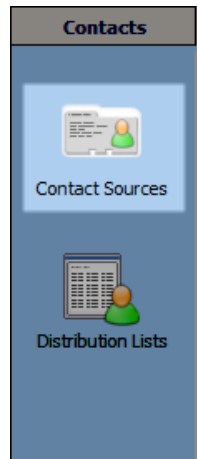
9. Confirm that the synchronization is successful and click OK to close the dialog.

Importing Contacts From a Vocera Voice Server Address Book

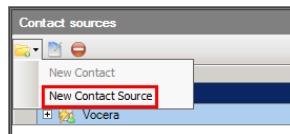
If you have stored contacts in an address book on the Vocera Voice Server, you can import them into VMP. This enables you to access these contacts from the VMP Web Console or Vocera Collaboration Suite.

To import contacts from a Vocera Voice Server address book:

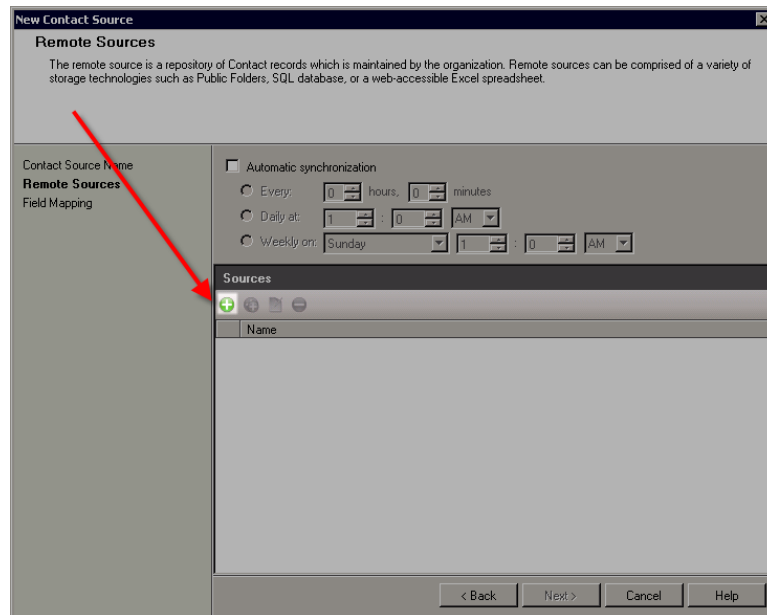
1. Select the **Contacts** module, and select **Contact Sources**.



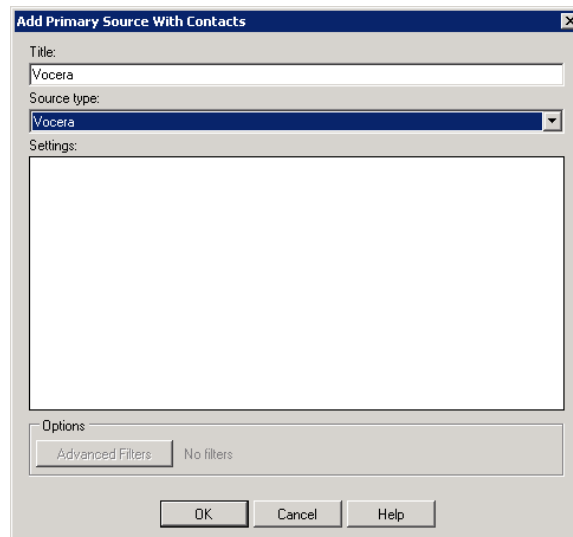
2. Select New and choose New Contact Source.



3. Enter a name for the new source, select the *Associated with remote source* checkbox, and click *Next*.
4. If you want the VMP Server to be synchronized with this source:
 - a. Select the *Automatic synchronization* checkbox.
 - b. Select whether you want to synchronize every few hours, daily, or weekly, and then select the time period or time at which synchronization is to take place.
5. If the Vocera source is not included in the list of contact sources, click *Add primary source with contacts*.



6. In the *Add Primary Source With Contacts* window, in the *Source type* dropdown list, select *Vocera*.



Add Primary Source With Contacts

Title: Vocera

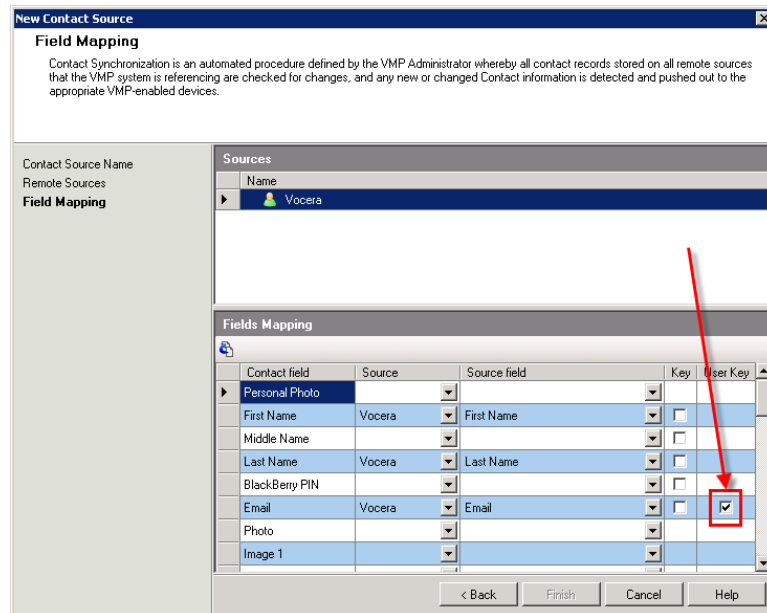
Source type: Vocera

Settings:

Options: No filters

Click OK. In the Remote Sources window, click Next. The Field Mapping window appears.

7. In the Field Mapping window, locate the Fields Mapping table at the bottom of the window. In the User Key column, ensure that the checkbox in the Email row is selected.



New Contact Source

Field Mapping

Contact Synchronization is an automated procedure defined by the VMP Administrator whereby all contact records stored on all remote sources that the VMP system is referencing are checked for changes, and any new or changed Contact information is detected and pushed out to the appropriate VMP-enabled devices.

Contact Source Name: Vocera

Remote Sources: Vocera

Field Mapping

Contact field	Source	Source field	Key	User Key
Personal Photo	Vocera	First Name	<input type="checkbox"/>	<input type="checkbox"/>
First Name	Vocera	Last Name	<input type="checkbox"/>	<input type="checkbox"/>
Middle Name	Vocera	BlackBerry PIN	<input type="checkbox"/>	<input type="checkbox"/>
Last Name	Vocera	Email	<input type="checkbox"/>	<input checked="" type="checkbox"/>
BlackBerry PIN	Vocera	Photo	<input type="checkbox"/>	<input type="checkbox"/>
Email	Vocera	Image 1	<input type="checkbox"/>	<input type="checkbox"/>
Photo	Vocera		<input type="checkbox"/>	<input type="checkbox"/>
Image 1	Vocera		<input type="checkbox"/>	<input type="checkbox"/>

< Back Finish Cancel Help

8. In the Key column, select the checkboxes in the First Name, Last Name, and Email rows, as shown below. Then, scroll down to Business Phone and select this checkbox also. These define the unique key that will be used to identify each address book entry.

New Contact Source

Field Mapping

Contact Synchronization is an automated procedure defined by the VMP Administrator whereby all contact records stored on all remote sources that the VMP system is referencing are checked for changes, and any new or changed Contact information is detected and pushed out to the appropriate VMP-enabled devices.

Contact Source Name
Remote Sources
Field Mapping

Sources

Name
Vocera

Fields Mapping

Contact field	Source	Source field	Key	User Key
Personal Photo				
First Name	Vocera	First Name	<input checked="" type="checkbox"/>	
Middle Name			<input type="checkbox"/>	
Last Name	Vocera	Last Name	<input checked="" type="checkbox"/>	
BlackBerry PIN			<input type="checkbox"/>	
Email	Vocera	Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Photo				
Image 1				

< Back Finish Cancel Help

If your site uses pagers, scroll to the Pager checkbox and select it also.

Setting these key entries is the best practice for most deployment models. Check your Vocera Voice Server address book to see what model works best for you.

9. Click Finish to start synchronizing the address book.
10. Confirm that the synchronization is successful and click OK to close the dialog.

Adding a Secondary Source

When synchronizing, you can specify a secondary source that is to be linked with data in one of the sources that you have previously created. To link a secondary source with a primary source, you must specify the common key between the two sources.

1. During synchronization, in the Remote Sources window, locate the Sources pane and click Add source with additional user info.

User Synchronization

Remote Sources

In the context of the User Synchronization, the remote source is a repository of User records which is maintained by the or data referenced from remote sources will include First, middle and last name, PIN and email.

Reconfigure/Synchronize only
Remote Sources
Select Users
User/DL Synchronization
Field Mapping
Script
Export Address Book Entries to Vocera

☐ Automatic synchronization
☐ Every: 0 hours, 0 minutes
☐ Daily at: 1 : 0 AM
☐ Weekly on: Sunday 1 : 0
☐ Auto Create and Delete users
☒ When a user's wireless gateway is not provided, use:
Vocera Smartphone client
☒ Merge primary sources

Sources

Name
Vocera
Active Directory

2. In the Add Source With Additional User Info dialog box, supply the title, source type, and connection parameters for the new secondary source. These fields are identical to those that you provide when you are creating a primary source.

Add Source With Additional User Info

Title:

Source type:

Connection parameters:

File path	
Login	
Password	
Confirm Password	
Worksheet	
Document contains columns title	Yes
Header row number	1
Contact row number	2

Options

Sources linkage

Source key field:

Parent source key field:

For details on providing these fields, see one of the following, depending on the type of the secondary source that you are creating:

- Active Directory: see [Importing Users From Active Directory](#) on page 51
 - Vocera Voice Server: see [Importing Users From Vocera Voice Server](#) on page 49
 - Excel and CSV files: see [Importing Users From an Excel or CSV File](#) on page 54
 - SQL: see [Importing Users From SQL](#) on page 56
3. In the **Source key field**, specify the secondary source field to use as the common key.
 4. In the **Parent source key field**, specify the primary source field to associate with the secondary source key field.
 5. Click **OK** to add the secondary source.

User Devices and Client Application Configuration

To enable user devices and client applications to work with the VMP Server, you can perform these tasks.

- Send device installation information to a user device.
- Set up autoconfiguration for Vocera Collaboration Suite devices.
- Enable or disable email communication on user devices and the VMP Web Console.

Vocera Solution Comparison

Vocera smartphone and badge solutions offer secure messaging capability to any health care professional. Regardless of role or location, you can use Vocera to send secure, HIPAA-compliant messages to any member of your care team.

The following table lists the attributes and capabilities of the Vocera badge, Vocera Secure Texting and Vocera Collaboration Suite. Use this table to determine what solution is the best choice for you.

Attribute	Vocera Badge	Vocera Secure Texting		Vocera Collaboration Suite	
Network Supported	Wi-Fi	Cellular	Wi-Fi	Cellular	Wi-Fi
Supports Shared Devices	✓			✓	✓
Hands Free	✓				
Voice Automated	✓			✓	✓
Contact by Name, Role, Group	✓	✓	✓	✓	✓
Receive Group Call and Broadcast	✓				✓
Initiate Group Call and Broadcast	✓			✓	✓
Push-to-Talk	✓				✓
Contacts Directory Search		✓	✓	✓	✓
Favorites List		✓	✓	✓	✓
Presence/Availability Information		✓	✓	✓	✓
Select-to-Connect Commands		✓	✓	✓	✓
Keypad for extension dialing				✓	✓

Attribute	Vocera Badge	Vocera Secure Texting	Vocera Collaboration Suite
Simple Paging	✓		✓
Alarms/Alerts through integration	✓		✓
Secure transmission and delivery of messages		✓	✓
Text Users and Groups		✓	✓
Web Console Messaging		✓	✓

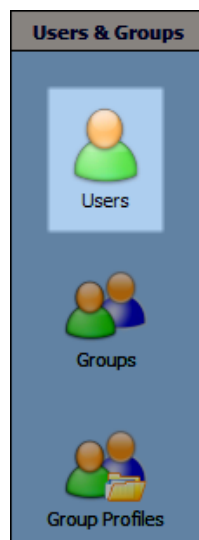
The Vocera messaging solutions enable you to:

- Reach the **right person, instantly**.
- At the **right time**.
- On the **right device**.
- With the **right information**.
- In the **right place, anywhere**.

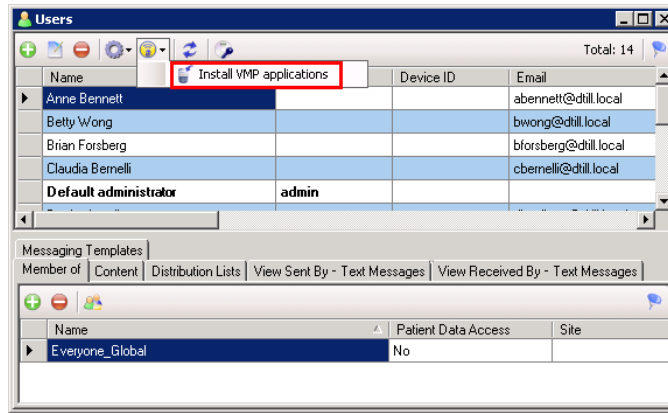
Sending Installation Information to User Devices

You can send instructions on how to install and register the client application on a user's device.

1. Select Users & Groups > Users.



2. In the Users pane, highlight the name of the user to be sent installation instructions.
3. In the toolbar, click the Notify mobile device dropdown list and select Install VMP applications.



4. If no registration key exists for this user, you will be asked whether you want to generate one. Click Yes.
5. A notification dialog box appears, indicating that the installation information has been sent to the user's email address.



Note: The generated registration key is valid for 48 hours only.

Autoconfiguration of Vocera Collaboration Suite Devices

When the Vocera Collaboration Suite is started on a device, a startup screen appears on which the user can specify the fully-qualified domain name (FQDN) or IP address of the VMP Server. You can autoconfigure the Vocera Collaboration Suite client to display the FQDN or IP address of the server on this startup screen.

To set up autoconfiguration, have your IT department create a DNS entry named `autodiscovervs` for the VMP Server. The recommended approach is to configure the `autodiscovervs` entry as a CNAME record and reference the FQDN of the VMP Server (or the VMP Server load balancer). The VCS client will use the FQDN present in the CNAME record if found. If no DNS CNAME record is found but an A record exists for `autodiscovervs`, the VCS client will use the IP address specified to connect to the VMP Server.

The VCS client will search for `autodiscovervs.localdevice` if it cannot find `autodiscovervs`.

Enabling Email Communication

You can configure the VMP Server to enable or disable email communication on user devices and the VMP Web Console.

1. Start the VMP Administrator and select **Configuration > System Options**.



The System Options dialog box appears.

2. Scroll to Contacts.
3. From the Allow Email Communication dropdown list, select Yes to allow clients to send email to contacts, or select No to disallow email.

System Options	
Auto Lock (in minutes, seconds)	1m
Enforce Change Password	Yes
Password Change frequency (in days)	120
Unique passwords before reuse permitted	2
Maximum failed attempts before device wipe	20
User Inactivity	
Time of inactivity for automatic logout (in minutes)	30
Days of inactivity before user is placed into Warning state	60
Days of inactivity before user is placed into Locked state	90
Time of inactivity for auto logout for smartphone client (in minutes)	60
Device inactivity timeout interval (in minutes)	10
VCS logout in dual mode also causes a badge logout	Yes
Contacts	
Allow User to upload personal image	Yes
Allow Email Communication	Yes
Secure Messaging	
Enable Remind Me Later Option	No
Default Subject Line for 3rd Party Integrations	3rd Party Notification
Description	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

4. Click OK to save your change.

Updating the APNS Certificates

The connection between the VMP Server and the Apple Push Notification Service (APNS) requires two security certificates. These certificates are included as part of the VMP Server installation process, and must be updated every year.

When the VMP Server wants to send a message or other notification to a device running Vocera Collaboration Suite on the iOS operating system and the device is not on the corporate network, it sends the notification to the APNS, which then sends the notification to the device. The APNS certificate enables the use of this notification method.

The APNS VoIP certificate enables VCS clients to use the Apple PushKit capability to receive push notifications.

When your existing certificates are about to expire, the VMP Server automatically downloads the new certificate files and updates your certificates, if this is possible. If the server cannot locate the updated certificates, it sends you an email message that warns you that your certificates are about to expire. The server also sends an email message if your certificates have expired.

To update your certificates:

1. Start the VMP Enterprise Manager.
2. From the **Tools** menu, select **Update VCS APNS certificate** to update the APNS certificate for the Vocera Collaboration Suite client.
3. Specify the location of the APNS certificate file that has been provided to you, and click **OK**.
4. From the **Tools** menu, select **Update VCS APNS VOIP certificate** to update the APNS certificate for VoIP for the Vocera Collaboration Suite client.
5. Specify the location of the APNS VoIP certificate file that has been provided to you, and click **OK**.

The certificates are now updated.



Important: Your server must allow access to *.vocera.com over port 443, or your APNS certificates will not be updated.

About Device Certificates

You can use a certificate-based solution to ensure that only trusted devices can use the Vocera Collaboration Suite application to connect to the VMP Server.

To employ this solution, contact your IT administrator and obtain a root and child certificate pair for use in your VMP and VCS environment. This certificate pair should not be used for any other purpose.

The root certificate is then installed on the VCS devices that are to be trusted. You can install this certificate in any of the following ways:

- Use a Mobile Device Management (MDM) solution. Ensure that your VCS devices can gain access to the certificate from the MDM.
- For Apple devices, use the Apple Configuration Utility.
- Provide a link to the certificate in an email message that is provided to devices as part of the device registration process.



Note: Each VCS device must have the same root certificate.

The child or leaf certificate of the root certificate is then installed on the VMP Server. See [Uploading a Device Certificate](#) on page 78 for details on how to install this child or leaf certificate.



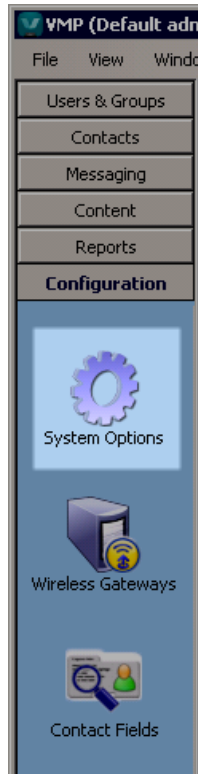
Note: For technical details on the certificate and public key pinning solution used here, see [Certificate and Public Key Pinning](#).

Uploading a Device Certificate

If you have used a Mobile Device Management solution or other solution to install a root certificate on your devices, you can provide a child or leaf certificate of this root certificate to the VMP Server. This ensures that only trusted devices can use the Vocera Collaboration Suite application to connect to the VMP Server.

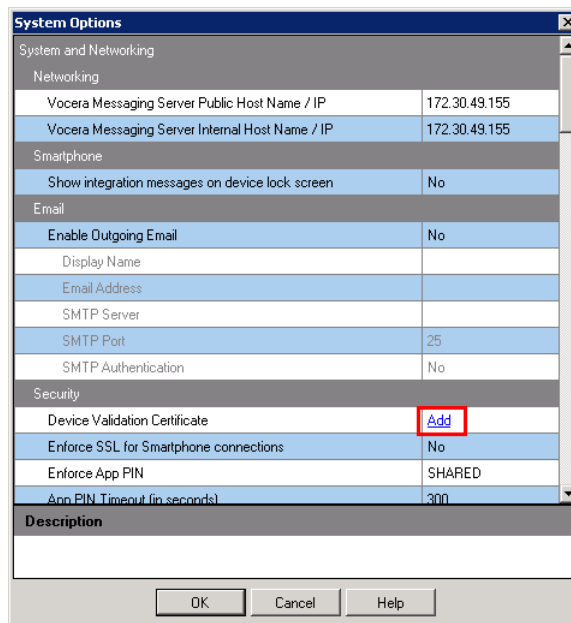
To upload a child or leaf certificate to the VMP Server:

1. Start the VMP Administrator and select **Configuration > System Options**.



The System Options dialog box appears.

2. In the System and Networking section, scroll to Security.
3. In the Device Validation Certificate row, click Add.



4. Locate the child or leaf certificate on your computer. The file name for this certificate has the suffix **.cer**.
5. Click **Open**. The device certificate is now uploaded.

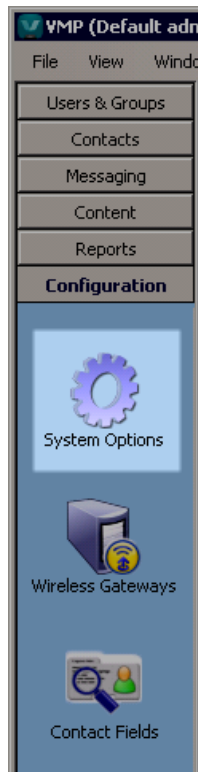
Configuring VCS to Use Vocera Client Gateway

You can specify that VCS is to use TCP to communicate with the Vocera Client Gateway server instead of using Comet to communicate with the Vocera Voice Server. This is recommended, as it improves resource management on the VCS clients.



Note: Vocera Voice Server 5.2.2 or later and VCS 3.2 or later are prerequisites if you want to use TCP to communicate with the Vocera Client Gateway server.

1. Start the VMP Administrator and select **Configuration > System Options**.



The System Options dialog box appears.

2. Scroll down to the **Integrations > Vocera Voice** section.
3. Set the **Use VCG for VCS client connection management** option to **Yes**.

System Options	
Organization Name	
Text	
Web Console Date Format	MMM/dd/yyyy
Enabled	Yes
Integrations	
Vocera Voice	
Enabled	Yes
IP Addresses	172.30.49.161
Port	80
Use HTTPS	No
VCG IP Addresses	
VMI Message Expiry (in minutes)	5
Enable Enhanced Voice Server NIO Tomcat Feature	No
Use VCG for VCS client connection management	Yes
Patient Context	
Enabled	Yes
Adapter URL	http://172.30.48.20...
Adapter Authentication Key	H6atVht-9UEmw6
Description	
When enabled the VCS client will use the VCG server for enhanced connection management. This setting is recommended to improve resource management on the clients. Requires VCG version 5.2.2 or higher and VCS version 3.2 or higher.	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

4. Click OK to save your changes.

On the Vocera Client Gateway server, you can edit a properties file named **vgwproperties.txt** to control the behavior of the VCS and VMP interface. For more details, see the *Vocera Voice Server Telephony Configuration Guide*.

Vocera Client Gateway Site Awareness

In a multi-site environment, the Vocera Collaboration Suite client provides information to the VMP Server to determine the location of the Vocera Client Gateway servers to use when making calls. This ensures that calls do not have to traverse multiple network hops.

When a VCS client first registers with the VMP Server, it presents information to the server to register the client's location. The VMP Server then determines which Vocera Client Gateway servers are closest to this client's location. If necessary, the VMP Server communicates with the Vocera Voice Server to obtain this location information.

After receiving this location information, the VCS client uses it to determine which Vocera Client Gateway server to use. If the closest Vocera Client Gateway server is unavailable, the next closest is used, until the list is exhausted.

If the Vocera Collaboration Suite client is an older version, and does not provide any location information, the VMP Server provides a default set of Vocera Client Gateway server addresses to use. This list of servers is configured in the VMP Server.

For more information on locations, see the documentation on locations in the *Vocera Voice Server Administration Console Guide*.

Wakeup Notifications for VCS Clients

The VMP Server sends wakeup notifications to clients that are offline or do not have a Vocera Voice Server ID, and that have not sent a **getpushdata** query to the server within the last 5 minutes and 15 seconds.

When the server sends a wakeup notification, it sends a VoIP notification to clients running version 3.2 of VCS on iOS or a GCM notification to clients running version 3.2 of VCS on Android. It sends a regular APNS or GCM message to clients running older versions of VCS.

If a VCS client is also a Vocera Voice Server user and is logged into the Vocera Voice Server, notification is handled by both the Vocera Client Gateway and the VMP Server.

VCS Wi-Fi Configuration Best Practices

Smartphones are a necessary tool in today's workplace. Vocera Collaboration Suite is an essential smartphone application that allows users to securely stay connected. This documentation lists considerations to take into account before designing and deploying Vocera Collaboration Suite (VCS) as part of your workflow solution.

Wi-Fi Supported Settings

The Wi-Fi settings listed here are supported.

Setting	Recommendation
Wi-Fi Quality (2.4 and 5 GHz will be different)	Voice Grade
2.4 or 5 GHz	5 GHz only
MDM	Supported
Phone Model / OS	iPhone 5 or later / iOS 9.0.1 or later
	Android - Test
SSID Priority Queue	Highest
VPN / Per App VPN	No
Captive Portal	No
Session Timeouts	None
Wireless Authentication	WPA2 PSK
	802.1X w/ 802.11k/r
Client Exclusion Policies	Disabled

Site Survey

Vocera Collaboration Suite includes a voice application which connects over Wi-Fi. For best results, a Voice grade wireless network must be designed, and a site survey must be completed to verify proper coverage for the frequency band it will be deployed on.

If you have badges running on 2.4 GHz and plan to run VCS on 5 GHz, the 5GHz must be validated. The radio characteristics and planning of 2.4 and 5GHz are very different. Sufficient coverage on the 2.4 GHz network does not mean adequate coverage for 5 GHz. In both cases, the requirements are to have -65dBm power coverage with an SNR of 25 at 50mW or lower AP power output wherever the devices will be utilized.

Smartphones

One of the most important considerations when deploying Vocera Collaboration Suite is the capability of the smartphone platform.

Most smartphones are consumer grade devices and are limited in their Wi-Fi capabilities. Improvements come with each generation of the phone. For the best user experience, use a phone released in 2014 or later. Improvements have come in three main areas:

- Wi-Fi Roaming
- Wi-Fi Security
- Battery Management

Deployment Models

There are three typical models of smartphone use in the enterprise: Corporate Owned, BYOD, and Mixed.

Corporate Owned

The corporate owned model allows the business to completely secure the device and restrict applications and use for business needs.

A Mobile Device Management (MDM) solution is highly recommended to deploy and control these devices. With an MDM, the smartphone can be completely locked down so users can only use the necessary resources.

BYOD

Many employees have personal smartphones and use them at work. The challenge with this model is that it is difficult to know if the BYOD phone will perform well.

Use of an MDM can be highly beneficial in making sure the device meets the minimum technical and security requirements.

WLAN Settings

Many Vocera deployments are likely to have a combination of Vocera Badges and smartphones with the Vocera Collaboration Suite client installed. This section discusses the best practices for deploying for this mixture.

Wireless Priority and Applications

This table provides a list of priority classes and their associated data types and applications.

Priority Class	Data Type	Application	Example
Voice	Voice only	Critical, voice only applications	Vocera Badges
Video	Video/mixed use	Latency sensitive, mixed voice/data	Smartphone running Vocera CS
Best Effort	Data	Data only applications	Web, email, chat
Background	Guest	Not business related	Guest chat, video, etc.

Quality of Service

In the wireless world, QoS is used to make sure the most important traffic will have priority over less sensitive traffic.

Voice traffic is sensitive to delays in audio delivery (latency) and to variations in the timing of the audio delivery (jitter). Voice over wireless is especially challenged because it is a shared medium. For the best user experience, all audio traffic must be tagged with the appropriate QoS markings on the wired infrastructure and be allocated to the appropriate wireless priority queue. The recommendations described here focus on wireless prioritization, as it is typically more constricted.



Tip: An important thing to remember about Quality of Service (QoS) is that it is only important if there is contention on the media. Traffic metering lights on freeway entrances are a type of quality of service. When there is no traffic on the freeway there is no need to restrict traffic coming on. When the freeway is very busy, the metering lights are used to restrict the cadence of adding more traffic. This restriction prevents the freeway from coming to a standstill.

Wireless prioritization is usually done at the SSID level. Vocera recommends that all voice only applications, such as the Vocera Badge, be allocated to the voice SSID.

Mixed use devices, such as smartphones running Vocera Collaboration Suite (VCS), should use an SSID with highest priority. Because the smartphone can only associate to one SSID, it cannot send voice packets to the voice SSID and other packets to a lower priority SSID. It allows VCS voice packets to have higher priority over other data traffic. The data packets from VCS will not impact voice quality on the voice only SSID.

All other data applications in the environment should use an SSID with Best Effort priority. Data applications typically use TCP and HTTP, which have protocol layer redundancy. Latency and jitter that would seriously impact a voice application have no discernable effect on data applications.

The Background priority should be used for traffic that is least important to business. While Guest access is important to patient and family satisfaction, it is less important than most business traffic. Care should be taken to provide a balance for guest access to the wireless network.

2.4 vs 5 GHz Frequency Bands

The current generation of Apple and Android smartphones contain Wi-Fi radios that support both the 2.4 and 5 GHz frequency bands.

The 2.4 GHz band is typically overutilized because there are fewer channels and it is used by more devices. It also has more common interference sources, such as microwave ovens, wireless security cameras, and Bluetooth devices.

It is highly recommended that VCS enabled smartphones be deployed on a voice quality 5GHz infrastructure only.

5GHz Channels and Dynamic Frequency Selection (DFS)

Depending on location, some channels may not be available in the 5GHz frequency band. Channel use is limited by each country's regulatory agency.

Some of the 5 GHz channels are sometimes not available, as other applications (primarily RADAR) have priority use. If the Wi-Fi is using one of these channels and the AP detects it is being used by RADAR, the AP will change channels. When this happens, the clients associated with that AP will be forced to look for another AP. If a voice call is active during the channel change, voice audio will be interrupted.

If your facility is near an airport or a weather station (common users of RADAR), you should disable DFS channels.

Security

Wireless security is an important consideration, especially when deploying a BYOD model.

Captive Portal

Wi-Fi Captive Portals require the user to log in through a web page before getting full access to the Wi-Fi network.

The granted access is usually for a limited time. When that time expires, you must login again through the web page.

A Captive Portal should not be used when deploying VCS. If it must be deployed, set the session timeout to longer than a shift so that users do not have to re-login during their shift.

Virtual Personal Network (VPN)

VPNs are typically used to create a secure connection to a network. Using a VPN with VCS is not recommended.

- The VCS client is already on a secure network. Unless the VCS client is on the guest network (not recommended), it is already secure.
- VPN can be computationally intensive, which may cause delay or jitter in the audio packets.

iOS 7 Per App VPN

With iOS 7, Apple introduced a way to initiate a VPN on a per-application basis. Unfortunately, the implementation limits traffic over the VPN tunnel to TCP and HTTP traffic.

VCS uses UDP for both audio and signaling, and therefore will not work over a Per App VPN.

802.1X

Before a smartphone can use the Wi-Fi network, it must associate with the network and be validated.

The easiest way to do this is to configure a key on the smartphone. After it is configured and when it comes on the network, or when it roams between APs, the smartphone uses the key to get on the network.

A more secure method is to use an Authentication server (such as RADIUS, IAS, ICS, AAA). Authentication uses the 802.1X protocol to validate the user by using an Extensible Authentication Protocol (EAP) type. There are many EAP types, but they are all similar in that they communicate to the Authentication server before allowing access to the network. While 802.1X and EAP are more secure, they take time to perform the authentication. The authentication can take several seconds and occurs when the device first comes on the network and every time the smartphone roams between APs. If a smartphone is in a VCS call while roaming, there could be several seconds of lost audio on each roam.

802.11k/r

If 802.1X is required, 802.11k/r must be used. 802.11k/r are protocols that improve the roaming times drastically when using 802.1X.

VMP Security

The following sections describe how security is implemented in the VMP environment.

Configuring the VMP Server For Secure Connections

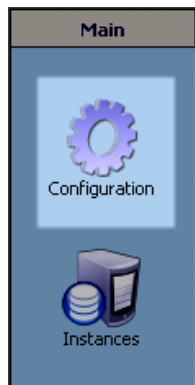
If the VMP Server was not configured to use SSL during installation, you can use the VMP Enterprise Manager to configure it to use SSL after installation.

You can also follow these steps to configure the VMP Server to use an updated SSL certificate.



Note: If you are using VMP in a clustered environment, and want to use SSL, you must configure each cluster node to use SSL.

1. Start the VMP Enterprise Manager.
2. Select Configuration.



The Configuration window appears.

3. Scroll down to the Services folder and then to the WDE subfolder.
4. In the NetworkSecureCertificate row, click in the Value column, then click select.

Services	
WDE	
NetworkInterface	0.0.0.0
NetworkPort	80
NetworkSecurePort	443
NetworkSecureCertificate	<input type="text" value="select"/>
NetworkSecureEnforceWebSSL	false
EnableWebServer	true

5. In the Select Certificate dialog box, select the SSL certificate that you want to use, and click OK.



Note: Vocera recommends that you use a publicly issued SSL certificate rather than a self-signed certificate. If a self-signed certificate is used, most web browsers will generate an error when the VMP Server is accessed from the VMP Web Console, which might cause confusion for end users.

6. If you want to enforce the use of SSL when connecting from a web browser to this VMP Server, click in the Value column of the NetworkSecureEnforceWebSSL row. From the

dropdown list that appears, select **true**. Users that attempt to connect using HTTP are now directed to the HTTPS URL.

Services	
WDE	
NetworkInterface	0.0.0.0
NetworkPort	80
NetworkSecurePort	443
NetworkSecureCertificate	
NetworkSecureEnforceWebSSL	false
EnableWebServer	true
Enable automatic Web login	true

For information on enforcing the use of SSL between the VMP Server and VMP clients, see [Enforcing SSL on the VMP Server](#) on page 86.

- Click **Save** to save your changes. In the confirmation dialog box that appears, click **OK**.
- After you have made your changes, the VMP Server needs to be restarted. In the dialog box that appears, click **Yes** to restart the VMP Server now, or click **No** to restart it later.

Enforcing SSL on the VMP Server

From the VMP Administrator, you can enforce that all communications between the VMP Server and VMP clients are to use SSL. This ensures that all communications are securely encrypted.

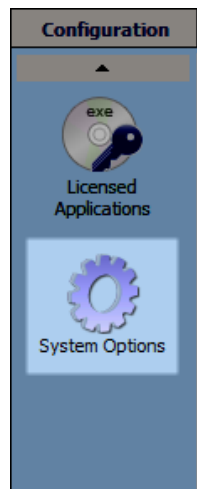


Note: The use of SSL can be enforced during the installation of the VMP Server. See [Installing the VMP Server](#) on page 13 for details.

If you are updating a previously installed VMP Server to enforce the use of SSL, all existing VMP clients that are not using SSL must re-register to use the VMP Server, as the connection protocol used by a client is specified when the client is registered.

Before you can enforce SSL use, you must configure a SSL certificate. For details, see [Configuring the VMP Server For Secure Connections](#) on page 85.

- Start the VMP Administrator.
- Select **Configuration > System Options**.



- In the System Options dialog box, scroll to the **Security** section and click in the right column of the **Enforce SSL for Smartphone connections** row.

System Options	
Networking	
Vocera Messaging Server Public Host Name / IP	172.30.49.159
Vocera Messaging Server Internal Host Name / IP	172.30.49.159
Email	
Enable Outgoing Email	No
Display Name	
Email Address	
SMTP Server	
SMTP Port	25
SMTP Authentication	No
Security	
Device Validation Certificate	Add
Enforce SSL for Smartphone connections	No
Enforce App PIN	OFF
App PIN Timeout (in seconds)	300
Enforce device password for all smartphones	No
Minimum Password Length	5
Require at least one letter	Yes
Description	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

4. From the dropdown list that appears, select Yes.
5. Click OK.

iOS and Android Security

For clients on the iOS and Android operating systems, the security and encryption structure depends on whether you are using the client within your organization's Wi-Fi network.

- Within the corporate Wi-Fi network, VMP uses Comet to send a content-less notification to the device. The device then accesses the VMP Server to retrieve the message.
- If you are using a device running the iOS operating system outside of your corporate Wi-Fi environment, the VMP Server uses the security features provided with the Apple Push Notification Service (APNS).
- If you are using a device running the Android operating system outside of your corporate Wi-Fi environment, the VMP Server uses the security features provided with the Google Cloud Messaging (GCM) service.



Note: On Android and iOS devices, the Vocera Collaboration Suite application performs its own data encryption and decryption. It does not depend on the operating system's encryption process.

Comet Notifications

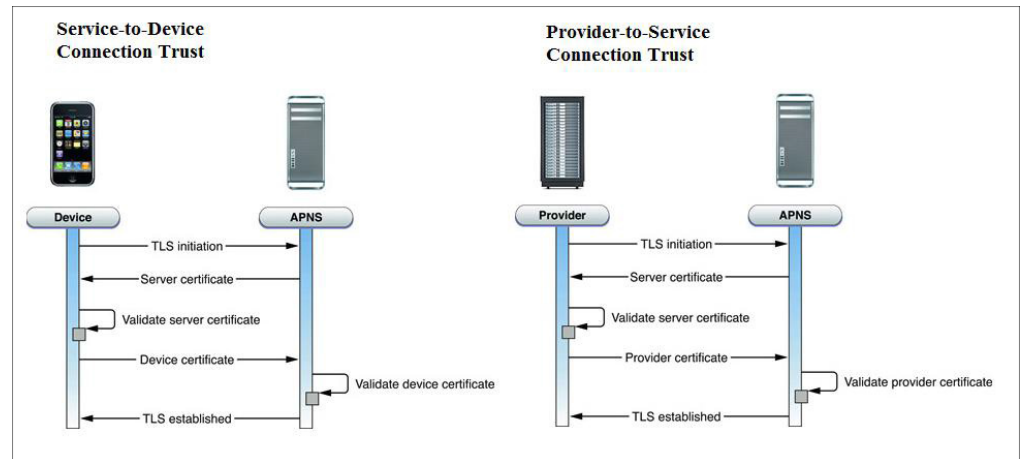
Older versions of the Vocera Collaboration Suite client on the iOS or Android operating system used Comet to send a content-less notification to the device when it was operating within the organization's Wi-Fi network.

This capability has been retained for backward compatibility, but Vocera recommends that you use a connection to the Vocera Client Gateway server instead. See [Configuring VCS to Use Vocera Client Gateway](#) on page 79 for more details.

Apple iOS Server Data Encryption

To enable communication between a provider and a device, the Apple Push Notification Service (APNS) must expose two standard ports (2195 and 2196). To ensure security, it must also regulate access to these entry points. For this purpose, APNS requires two different levels of trust for providers, devices, and their communications. These are known as connection trust and token trust.

- Connection trust establishes certainty that, on one side, the APNS connection is with an authorized provider with whom Apple has agreed to deliver notifications. On the device side of the connection, APNS must validate that the connection is with a legitimate device.
- Token trust is made possible through the device token. A device token is an opaque identifier of a device that APNS gives to the device when it first connects with it. The device shares the device token with its provider. Thereafter, this token accompanies each notification from the provider. It is the basis for establishing trust that the routing of a particular notification is legitimate. In a metaphorical sense, it has the same function as a phone number, identifying the destination of a communication.



Apple APNS Data Transfer Encryption

Apple Push Notification Service (APNS) is a robust and highly efficient service for sending secure data to devices running on the iOS operating system. Each device establishes an accredited and encrypted IP connection with the service and receives notifications over this persistent connection. If a notification for an application arrives when that application is not running, the device alerts the user that the application has data waiting for it.

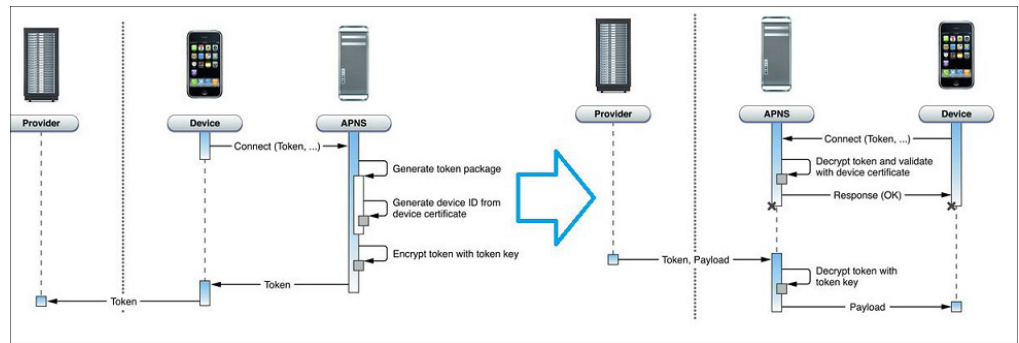
APNS includes a default Quality of Service (QoS) component that performs a store-and-forward function. If APNS attempts to deliver a message when the device is offline, the QoS stores the notification. It retains only one notification per application on a device: the last notification received from a provider for that application. When the offline device later reconnects, the QoS forwards the stored notification to the device. The QoS retains a notification for a limited period before deleting it.

Apple iOS Device Data Encryption

All devices using Vocera Collaboration Suite with iOS must register with the VMP Server to receive push notifications. The registration occurs after the application is installed.

Once iOS receives the registration request from an application, it connects with APNS and forwards the request. APNS generates a device token using information contained in the unique device certificate. The device token contains an identifier of the device. It then encrypts the device token with a token key and returns it to the device.

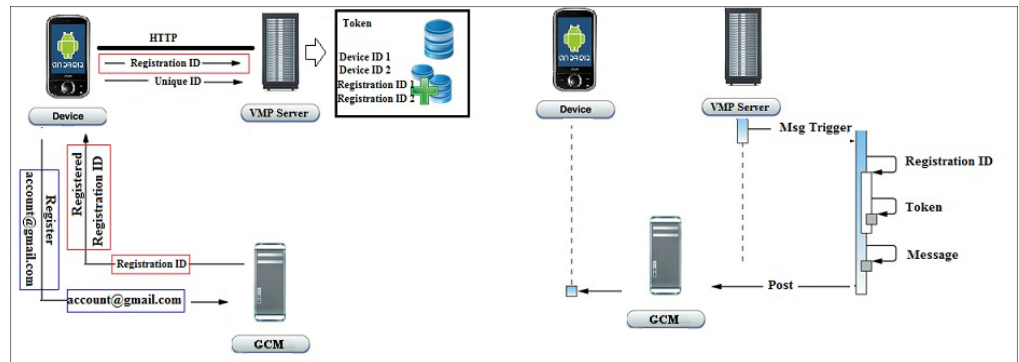
The diagram below shows the token relationship between the VMP Server, APNS, and the client device.



Android Server Data Encryption

The VMP Server needs to authenticate itself with the GCM. This is done via an authentication token that is determined with an HTTP POST request to the GCM servers.

The token is stored on the VMP Server and is used to authenticate the application server with the GCM servers once it sends out data. In a GCM, you have three involved parties: the VMP Server that wants to push messages to the Android device, the Google GCM servers, and the Vocera Collaboration Suite client application.



For the server to send a message, the application must have a registration ID that allows it to receive messages for a particular device. The registration keys are securely stored within the SQL database.

The ClientLogin token authorizes the server to send encrypted data to the client application on the Android device. The server has one ClientLogin token and multiple registration IDs. Each registration ID represents a particular device that has registered to use the messaging service for Vocera Collaboration Suite.

When the VMP Server sends data, the following occurs:

1. The VMP Server sends data to the GCM servers.
2. Google queues and stores the message in case the device is inactive.
3. When the device is online, Google sends the message to the device.
4. On the device, the system broadcasts the message to the specified application via Intent broadcast with proper permissions, so that only the targeted application gets the message. This wakes the application up. The application does not need to be running beforehand to receive the message.
5. The application processes the secure data.

This is the sequence of events that occurs when an Android application running on a mobile device receives a message:

1. The system receives the incoming message and extracts the raw key/value pairs from the message payload.

2. The system passes the key/value pairs to Vocera Collaboration Suite.
3. The Android application extracts the raw data from the RECEIVE Intent by key and processes the data.

Android GCM Device Data Encryption

The Android-based Vocera Collaboration Suite application must register with the VMP Server to receive push notifications. It does this right after it is installed on a device.

The Android mobile OS receives the registration request from an application, connects with GCM, and forwards the request to the server. GCM generates a device token using information contained in the unique device certificate. The device token contains an identifier of the device. It then encrypts the device token with a token key and returns it to the device.

Enforcing Password Use

The VMP Server provides configuration options to ensure that all smartphone users are required to protect the device with a password. This option ensures that your confidential internal information is protected if the device is lost or stolen.

You can also specify that Vocera Collaboration Suite users must provide a four-digit Personal Identification Number (PIN) when accessing the app on either shared devices or all devices.



Tip: When configuring password options, remember to consider the speed at which your users must view and respond to critical communications. An auto-lock setting that is too short will impair the user's ability to quickly respond to messages and communications. A password that requires too many characters may also be inhibiting, depending on the environment.

1. Start the VMP Administrator: All Programs > VMP > VMP Administrator
2. Type **admin** (or your administrative credentials) in the VMP Login dialog, and click OK.
3. Select Configuration > System Options.



The System Options dialog box appears.

4. Scroll to Security > Enable device password for all smartphones, and select Yes.

System Options	
SMTP Server	
SMTP Port	25
SMTP Authentication	No
Security	
Device Validation Certificate	Add
Enforce SSL for Smartphone connections	No
Enforce App PIN	SHARED
App PIN Timeout (in seconds)	300
Enforce device password for all smartphones	Yes
Minimum Password Length	5
Require at least one letter	Yes
Auto Lock (in minutes, seconds)	1m
Enforce Change Password	Yes
Password Change frequency (in days)	120
Unique passwords before reuse permitted	2
Maximum failed attempts before device wipe	20
Accept client log uploads	Yes
User Inactivity	
Description	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

5. Configure the following options:

Table 21: Device password configuration options

Option	Description
Minimum Password Length	Enter the number of characters the user must include in the device password. For iPhone users, the device Passcode Lock settings must be changed if you want a password longer than 4 numerical digits.
Require at least one letter	Select Yes to ensure that the user adds at least one letter to the device password. For iPhone users, you cannot insist on a password with at least one letter. For iPhone users, the device Passcode Lock settings must be changed if you want a password to include a letter.
Auto Lock	Set the duration of inactivity, in minutes and seconds, until the device auto-locks. In the following example, the device is set to auto-lock after five minutes and thirty seconds: 5m30
Enforce Change Password	Select Yes to ensure the user changes the device password at a regular frequency.
Password Change frequency	If Enforce change password is set to Yes, enter the interval, in days, at which the user is required to change the device password.
Unique passwords before reuse permitted	The VMP Server stores a list of the most recently used passwords for a device. A password cannot be reused if it is one of the <i>N</i> most recent passwords used, where <i>N</i> is the value of this option.
Maximum failed attempts before device wipe	Enter the number of times a password can be incorrectly entered before all system sensitive information is wiped from the device.

6. Set the Enforce App PIN option to one of the following:
- OFF: Do not require the use of a PIN when accessing the Vocera Collaboration Suite.
 - SHARED: Require the use of a PIN on shared devices only.
 - ON: Require all users to supply a PIN. Users of personal devices must have their username and password credentials to supply the PIN, or they will be locked out of the Vocera Collaboration Suite application.
7. If Enforce App PIN has been selected, set App PIN Timeout to the amount of time, in seconds, that the device can remain idle before the PIN must be entered again.



Note: If you change the Enforce App PIN setting to ON, device users will not be able to set a PIN if they registered by email or using a registration key and do not have either a valid VMP Server username and password or a valid Active Directory username and password.

Remote Wipe

Vocera Messaging Platform provides a data wipe option to let you remove sensitive Vocera data from the mobile device without affecting any other mobile data. Additionally, if a more in-depth device wipe is required, leveraging Microsoft Exchange or a Mobile Device Management tool may be effective.

This is useful when a user is no longer employed by the organization, a device is lost or stolen, a shared device is assigned to a new user, or in the event of a communicated security breach.

Performing a Remote Wipe from the VMP Administrator

You can use the VMP Administrator to wipe sensitive Vocera data from the device.

1. Select the Users & Groups module, and click to highlight the user to remove.
2. Select the **Delete** button. A window will prompt the administrator to remotely wipe the data from the smartphone. Once complete, the user account will be inactive on the server, and VMP data will be removed from the user's device.

Performing Remote Wipe Using Microsoft Exchange

If you have an iOS or Android device, you can use Microsoft Exchange to wipe sensitive Vocera data from it.

1. In the console tree, navigate to **Recipient Configuration > Mailbox**.
2. Select the user from the Mailbox window.
3. In the action pane, click **Manage mobile device**, or right-click the user's mailbox, and click **Manage mobile device**.
4. Select the mobile phone.
5. In the **Actions** section, click **Clear**, and click **Clear** again.

Performing Remote Wipe Using Outlook Web

You can use Outlook Web to wipe sensitive Vocera data from an Android or iOS device.



Note: This process is specific to iOS or Android devices.

1. Open the Outlook Web Application in a browser.
2. Sign in to the device owner's mailbox, and click **Options**.
3. In the Navigation Pane, select **Phone**.
4. Click the **Mobile Phones** tab.
5. Select the ID of the mobile phone that you want to wipe and remove from the list.
6. Click **Wipe device** and click **OK**.
7. Click **Remove Device**.

Performing Remote Wipe Using a Mobile Device Management Solution

You can use a Mobile Device Management (MDM) solution to wipe sensitive Vocera data from your device.

1. Submit a wipe request through the console, MDM Shell, or Self Service Portal. Submit the request as a **Wipe Now** command stored in a central database to be picked up by the device within a determined time in travel.
2. The device receives this Alert and immediately starts a management session with the Device Management server.
3. The device picks up its wipe request from the Device Management server, sends back an acknowledgement that started the wipe, and starts the wipe process.

Performing an Exchange Management Shell Remote Wipe

You can remove sensitive Vocera data from your device using an Exchange Management Shell (ECS) remote wipe.

1. Send a **Get-ActiveSyncDeviceStatistics** command, using the following syntax, where **name** is the user id:
`Get-ActiveSyncDeviceStatistics - Mailbox name | fl Identity`
2. Send a **Clear-ActiveSyncDevice** command, using the following syntax, where **name** is the user id:
`Clear-ActiveSyncDevice -Identity WM_name`

High Availability and VMP

The Vocera Messaging Platform is designed to support clustered environments using active server and passive server configuration.

In a clustered environment, the primary server:

- Routes system traffic.
- Responds to the load balancer acknowledgment request every ten seconds.
- Updates the SQL server timestamp every two seconds.

Secondary nodes retrieve a timestamp from the SQL server every two seconds, but stay passive unless the primary node has not updated the SQL server timestamp in the last 20 seconds, at which point the primary node is assumed to have failed. The load balancer manages the status of each VMP Server by sending a health check request to the primary and secondary nodes. The load balancer redirects traffic to a secondary node after a third missed heartbeat from the primary node.



Note: For instructions on how to install VMP on a cluster, see [VMP Cluster Installation](#) on page 22.



Tip: Configure email alert notifications to receive an alert when a failover occurs. For details, see [Configuring Failover Email Notifications](#) on page 95.

Failover Configuration

A typical failover configuration consists of a primary and secondary VMP Server, a load balancer, and a SQL server.

This table shows the behavior of each of these server nodes.

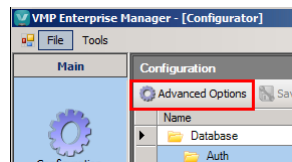
Node	Description
Primary Vocera Messaging Platform (VMP Server 1)	<ul style="list-style-type: none">• The primary server is accepting all HTTPS traffic.• The primary server is responding with a positive acknowledgment request from the Load Balancer every 10 seconds.• The primary server is updating the SQL server with a timestamp every 2 seconds.
Secondary Vocera Messaging Platform (VMP Server 2)	<ul style="list-style-type: none">• The secondary server is the standby server.• The secondary server is not responding with a positive acknowledgment request from the Load Balancer every 10 seconds.• The secondary server is retrieving a timestamp from the SQL server every 2 seconds. <p>If the SQL timestamp table has not been updated by VMP Server 1 within 20 seconds, VMP Server 2 will automatically start its HTTP interface and begin to accept traffic from the Load Balancer.</p>

Node	Description
The Load Balancer in conjunction with the VMP Server pair	<ul style="list-style-type: none"> The Load Balancer is sending an HTTP health check request to both VMP Server 1 and VMP Server 2. After a third response failure from VMP Server 1, the Load Balancer will start routing traffic to VMP Server 2 (This will happen once VMP Server 2 has initialized its HTTP interface and is accepting requests.).
The SQL Server in conjunction with the VMP Server pair	<ul style="list-style-type: none"> VMP Server 1 is updating a timestamp in the SQL Timestamp Table every 2 seconds. VMP Server 2 is retrieving the timestamp from the SQL Timestamp Table every 2 seconds.

Configuring Failover Email Notifications

You can use the VMP Enterprise Manager to specify where an email notification is to be sent if a failover occurs.

- From the VMP Server, start the VMP Enterprise Manager:
Start > All Programs > VMP > VMP Enterprise Manager
- Select Configuration > Advanced Options.



- In the SMTP section, type the SMTP mail settings for your deployment.

SMTP	
Server	dev.vocera.com
Port	25
VMP email	techpubs@dev.vocera.com

- In the Logging section, type the notification email address.

ConnectionsLimit	4
Logging	
Limit log messages to VMP Log File	Write all events
Limit log messages to Windows Event Log	Errors
Limit EMail notifications	Do not notify
Email Address(es) for Notifications	techpubs@dev.vocera.com
Enable extended communication logging	true
Enable smartphone extended communication logging	false
Enable web console extended communication logging	false

If a failover occurs, the following email is sent:

Message from the VMP server: VMP SERVER2

VMP SERVER2 server becomes active application server

Post Failover Configuration

When a failover occurs, the secondary VMP Server takes over the role of the primary server.

The behavior of the two servers is shown below.

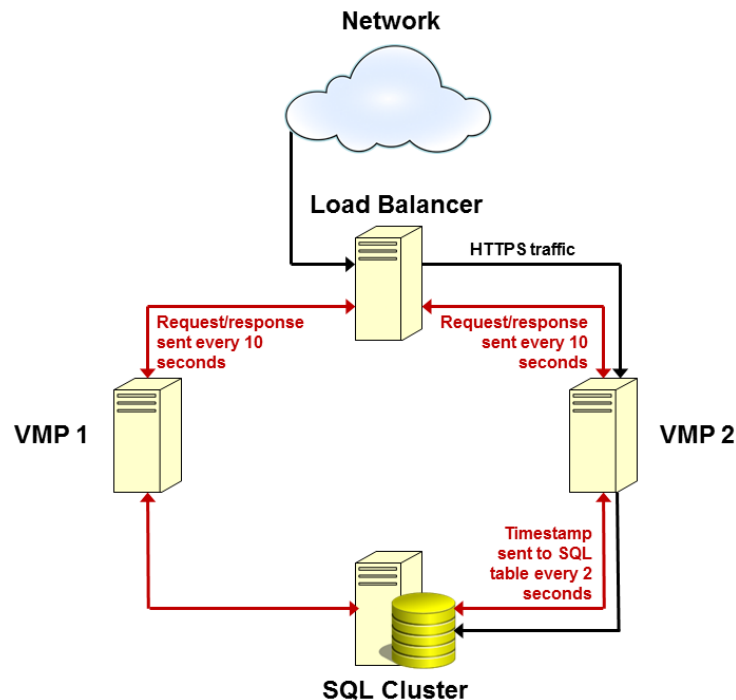
Primary VMP Server - VMP Server 1

- VMP Server 1 is now the secondary (passive) server.
- VMP Server 1 will attempt to send an E-Mail to the Administrator to indicate that a failover has occurred.

Secondary VMP Server - VMP Server 2

- VMP Server 2 is the primary (active) server and is accepting HTTPS traffic from the load balancer.
- VMP Server 2 will send an email to the administrator indicating its primary server status.
- VMP Server 2 is updating the SQL server with a timestamp every 2 seconds.

The Load Balancer is working in conjunction with the VMP Server pair, and is now redirecting all HTTPS traffic to VMP Server 2.



Restarting the Primary Server After Failover

When a failover has occurred, the Load Balancer is now directing the HTTPS traffic to the secondary VMP Server (VMP Server 2). You can reconfigure your environment so that traffic is directed to the primary server.

After this action has started, the Administrator will receive an email indicating that VMP Server 2 has become the primary server.

To reconfigure VMP Server 1 to be the primary server:

1. Shut down the Vocera Data Exchange Windows service on VMP Server 2.
2. Restart the Vocera Data Exchange Windows service on VMP Server 1. VMP Server 1 will assume primary server status.
3. Restart the Vocera Data Exchange Windows service on VMP Server 2. VMP Server 2 will assume secondary server status.

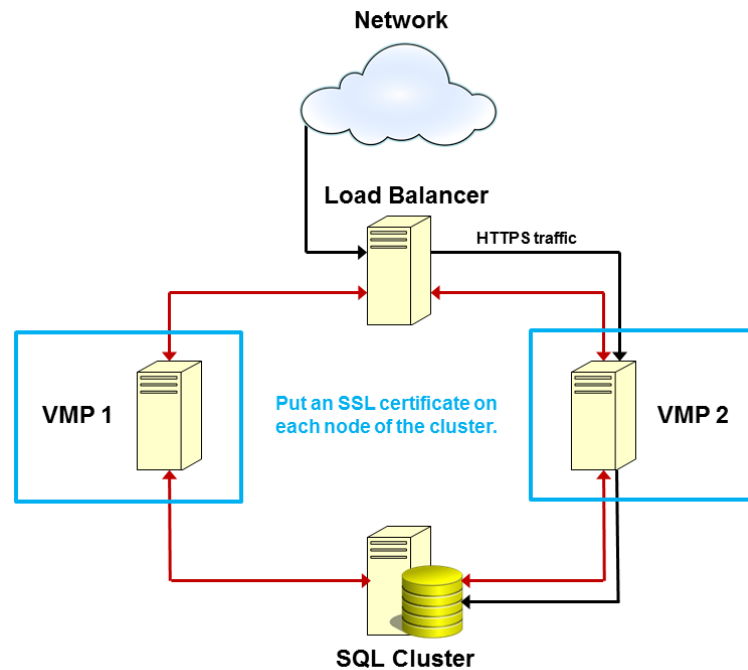


Note: If VMP Server 1 is to remain as the secondary server, no action is required.

SSL in a VMP Failover Environment

If you want to use SSL in a clustered VMP Server environment, Vocera recommends that you put an SSL certificate on each node on which a VMP Server is running. This ensures that all internal

traffic between the Load Balancer and each of the individual servers is secure, which may be a requirement in your jurisdiction if you are transmitting patient information.



Tip: Although a self-signed certificate is supported, it is best to use a publicly-registered SSL certificate for each VMP Server in your cluster.

To determine whether you need an SSL certificate for your Load Balancer to ensure end-to-end encryption, consult the specifications provided by the manufacturer of the Load Balancer.

Using SQL AlwaysOn Availability Groups and Failover Cluster Instances

SQL AlwaysOn Availability Groups and SQL AlwaysOn Failover Cluster Instances are high availability and disaster recovery solutions that provide an enterprise-level alternative to database mirroring.

SQL AlwaysOn Availability Groups is available for SQL Server 2012 and later, and SQL AlwaysOn Failover Cluster Instances is available for SQL Server 2014 and later.

An AlwaysOn Availability Group supports a failover environment for a discrete set of user databases, known as availability databases, that fail over together. The availability group supports a set of read-write primary databases and one to four sets of corresponding secondary databases.

An AlwaysOn Availability Instance supports a failover environment for a complete SQL instance, known as a failover cluster instance. When one instance fails, the secondary instance is activated. Refer to the Microsoft SQL documentation for information on how many secondary instances you can create in your environment.



Note: We do not support multiple listeners on different subnets in an AlwaysOn environment. This is because the .NET 3.5 SQL client does not support the multi-subnet capability.

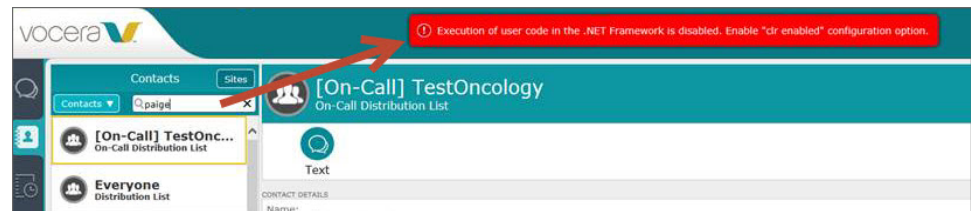
To set up an AlwaysOn Availability Group for VMP:

1. In each secondary database in the availability group, create the login names `wicauth` and `wicapplication`. These are the accounts that are created when the VMP Server is first installed.

The password for each of these accounts must be identical to the passwords specified during VMP installation. If the passwords are changed on the primary SQL server, they must also be changed on the secondary databases.

2. Link the `wicauth` and `wicapplication` accounts on each secondary database to the equivalent accounts in the WICMASTER database on the primary SQL server.
3. Enable CLR (Common Language Runtime) for each secondary instance of SQL.
4. Create an Assembly for each SQL instance. The VMP Web Console uses this Assembly for contact searches.

If CLR is not enabled and the Assembly is not created, the VMP Web Console displays the following error message when a secondary database becomes the primary:



Note: Contact Vocera technical support to obtain SQL scripts that will create the `wicauth` and `wicapplication` accounts, enable CLR, and create an Assembly for each secondary SQL instance.

To set up an AlwaysOn Failover Cluster Instance for VMP, no specific VMP-related configuration is required.



Wireless Gateway and Email Configuration

Learn how to configure wireless gateways and email connections in VMP.

Wireless Gateway Configuration

You can configure the SNPP and WCTP wireless gateways for VMP.

SNPP Gateways

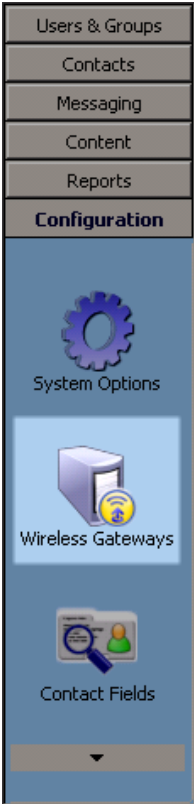
The SNPP protocol facilitates a link between the Internet and a TAP-compliant paging terminal. To configure VMP for use with a provider using SNPP, you must have the provider's SNPP address and port number.

For a list of provider SNPP addresses and port numbers, see [Note Page - Simple Network Paging Protocol \(SNPP\)](#).

Configuring an SNPP Wireless Gateway

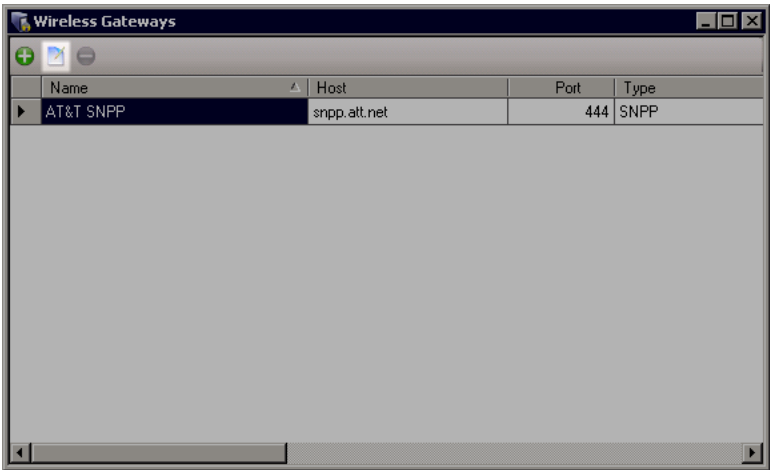
For a deployment with SNPP protocol, you can use the VMP Administrator to configure the SNPP Wireless Gateway.

1. Start the VMP Administrator application:
All Programs > VMP > VMP Administrator
2. Type **admin** (or your administrative credentials) in the VMP Login dialog, and click OK.
3. Select Configuration > Wireless Gateways.



The Wireless Gateways window appears.

4. Click to highlight AT&T SNPP, and click Edit.



5. Select the SNPP Implementation from the dropdown list.
ATT, Sprint, and Verizon are pre-configured. For another implementation, select Generic and provide the following details:

Table 22: SNPP Configuration Options

Option	Values
Name	Name the SNPP implementation.
Secure delivery	Select this option if the channel is secure and the full message content can be delivered. If this option is not selected, only the message subject is delivered.
Host	Enter the host name.
Port	Specify the port number to use.

Option	Values
SNPP gateway compatibility	Select One way or Two way from the dropdown list.
Max # of characters per message	Enter the maximum number of characters allowed in a text message.
Delivery receipts	Select to activate delivery receipts if this option is supported by the provider.
Treat "accepted by gateway" as delivery receipt	Select this option if it is supported by the provider. If this option is selected, the message is deemed delivered when accepted by the gateway.
Multiple Choice responses	This option is selected by default. Leave this option active unless instructed otherwise by the provider.
Use authentication	If authentication is required to establish the gateway connection, click to activate this option and enter the login credentials.

New Wireless Gateway

Name:

Type: **SNPP**

☒ Secure delivery

SNPP Implementation: **Generic**

Host: Port: **444**

Supported Features

SNPP gateway compatibility: **Two way**

Max # of characters per message:

☐ Delivery receipts

☐ Treat "accepted by gateway" as delivery receipt

☒ Multiple choice responses

☐ Use authentication

Login:

Password:

Confirmation:

OK Cancel Help

Configuring WCTP Polling

VMP supports polling to add additional features to AT&T Enterprise Paging, Sprint SMS, and US messaging gateways. Polling sends messages to the gateway at a set interval in order to determine if the page is sent, delivered, and read.

Use the following steps to configure polling for WCTP.

1. Start the VMP Administrator.
2. Select **Configuration > System Options**.



The System Options dialog box appears.

3. Scroll down to WCTP, enter the polling IDs, and click OK.

Inbound Integration

Learn how to integrate inbound WCTP, SOAP, or email connections to the VMP Server.



Note: By default, VMP licenses do not include access to the WCTP or SOAP connectors. See [Configuring the VMP License](#) on page 19 for more details.

WCTP Connections

VMP supports inbound WCTP messages from external systems, and forwards these messages to end-users' mobile devices.

Messages are delivered from VMP to:

- Supported iOS devices
- Supported Android smartphones
- Cellphones (via SMS)
- Pagers (via SNPP)
- Vocera badges

Delivery receipts, read receipts, text responses, and multiple choice responses are supported.

The WCTP request sent to the VMP Server sets the appropriate flags to **true** as per the specification, and the VMP Server provides the response to the initiating system. The VMP Server posts these responses and read/delivery receipts back to the originating system in real time.

The VMP SOAP-based API provides support for external systems to send messages, and to receive delivery statuses and responses to the messages (see the *Vocera Messaging Platform API Guide* for details).

Systems that support WCTP generally allow the administrator to identify users in the system as WCTP users, and point the WCTP configuration to the VMP Server. When a message needs to be sent, the system will send the message via the WCTP protocol to the VMP Server.



Note: USA Mobility is supported via outbound WCTP through a direct push rather than polling.

To configure WCTP, the third party needs the VMP Server URL with `/wctp?F=XX` appended. The format follows:

`www.domain.com/wctp?F=XX`

XX refers to the third-party system initiating the messages. The configuration is shown in the following code sample:

F=EM	For Emergen
F=generic	For all other systems (including Connexall)

To override the end user's profile settings, based on the priority of the message sent, append one or more of the following additional tags to the URL. Each tag can be set to Y (override) or N (do not override).

Tag	Description
&OH	Whether to override the user profile when the priority is High.
&ON	Whether to override the user profile when the priority is Normal.
&OL	Whether to override the user profile when the priority is Low.

The priority of the VMP message depends on these settings and on the priority of the message payload, as shown in the table below.

Priority appended to URL	Message payload priority	Resulting VMP message priority
	High	High
	Normal	Normal
&OH=Y	High	Urgent
&OH=Y	Normal	Normal
&OH=N	High	High
&OH=N	Normal	Normal
&ON=Y	High	High
&ON=Y	Normal	Normal
&ON=N	High	High
&ON=N	Normal	Normal
&OL=Y	High	High
&OL=Y	Normal	Normal
&OL=N	High	High
&OL=N	Normal	Normal

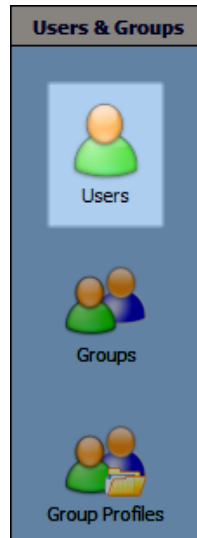


Note: These settings are supported on the Vocera Collaboration Suite and other Vocera smartphone clients.

Linking VMP with the WCTP Source

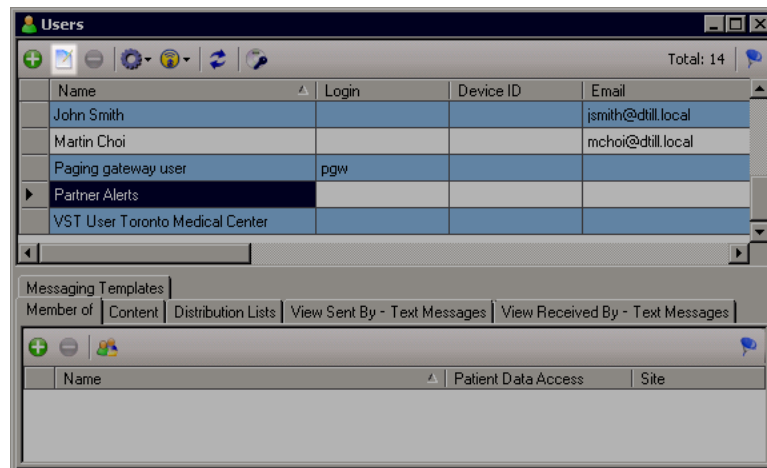
To link users with a WCTP source, a user must be created to support WCTP. This user account will send the messages.

1. Start the VMP Administrator.
2. Select Users & Groups > Users.

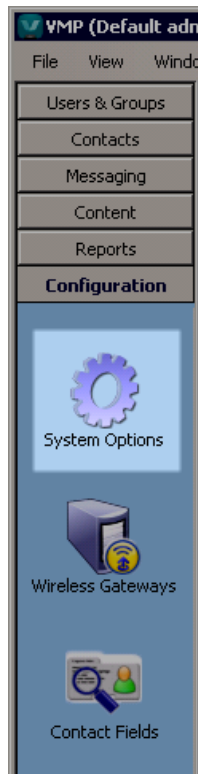


The Users window appears.

3. Click to highlight the Partner Alerts entry, and click Edit.



4. Specify a name that is relevant for your deployment. This is the name that appears as the sender for messages sent via WCTP.
5. Click Next, and click Finish.
6. Select Configuration > System Options.



The System Options dialog box appears.

7. Scroll down to the Default Subject for 3rd Party Integrations entry, change the subject line as appropriate for your deployment, and click OK.

System Options	
VCS logout in dual mode also causes a badge logout	Yes
Contacts	
Allow User to upload personal image	Yes
Allow Email Communication	Yes
Secure Messaging	
Enable Remind Me Later Option	No
Default Subject Line for 3rd Party Integrations	3rd Party Notification
Response waiting interval (in seconds)	600
Retain Message History in Database (in weeks)	104
Deliver message content to SMS users	Yes
Allow Urgent messages	Yes
Include attached images in the report	No
Number of days of inactivity to archive a conversation (in days)	14
Allow users to forward messages	Yes
Forward clinical system messages	No
Override Notifications	
Enable Do Not Disturb Mode on Smartphone Clients	Yes
Content	
Description	

OK Cancel Help

If a WCTP message starts with the text **Subject:**, VMP uses the rest of the line containing this text as the subject field for the message. VMP then skips one empty line and extracts the remaining data as the body of the message.

The following is a simple example of a WCTP XML payload that overrides the default subject:

```
<?xml version="1.0"?>
<!DOCTYPE wctp-Operation SYSTEM "http://dtd.wctp.org/wctp-dtd-v1r1.dtd">
<wctp-Operation wctpVersion="wctp-dtd-v1r1">
  <wctp-SubmitRequest>
```

```

<wctp-SubmitHeader submitTimestamp="2010-03-31T01:00:56">
  <wctp-Originator senderID="166.214.43.65:8088/WCTP"
    securityCode=""/>
  <wctp-MessageControl messageID="5345-21" transactionID="5345-21"
    allowResponse="false" notifyWhenDelivered="false"
    deliveryPriority="HIGH" preformatted="true"/>
  <wctp-Recipient recipientID="12345"/>
</wctp-SubmitHeader>
<wctp-Payload>
  <wctp-Alphanumeric>Subject: This is a subject.

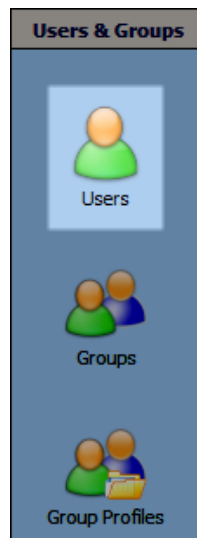
  This is a message body</wctp-Alphanumeric>
</wctp-Payload>
</wctp-SubmitRequest>
</wctp-Operation>

```

Configuring the VMP User to Receive WCTP Messages

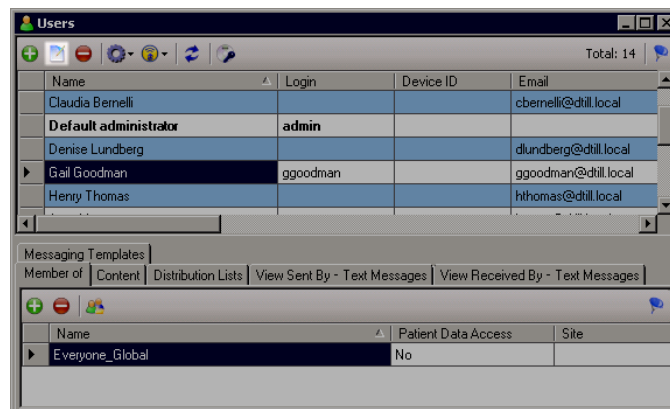
Users that are configured to receive WCTP messages can be set up manually using the VMP Administrator, or the VMP Server can connect to a SQL table and synchronize this information on a regular schedule.

1. Start the VMP Administrator.
2. Select Users & Groups > Users.



The Users window appears.

3. Click to highlight the user that is to be configured to receive WCTP messages, and click Edit.



4. Enter a value in the Public ID field or the Pager ID field to match the WCTP Source recipientID.

Edit User

Step 1: End-User Settings

Step 1: End-User Settings
Step 2: Push Technology and Licensing

First Name:

Middle Name:

Last Name:

Title:

Email:

Public ID:

Pager ID:

Vocera ID:

Home Site:

Auto Forwarding

Allow Forwarding:

Forward To:

Desktop and Web Access

☐ Enable PC Admin Console Access

☒ Enable Web Console Access

Vocera credentials

Login:

Password:

Confirmation:



Note: The WCTP Source can identify the recipient using a phone number, email address, or randomly generated number. The only requirement is that it must match the user Pager ID field.

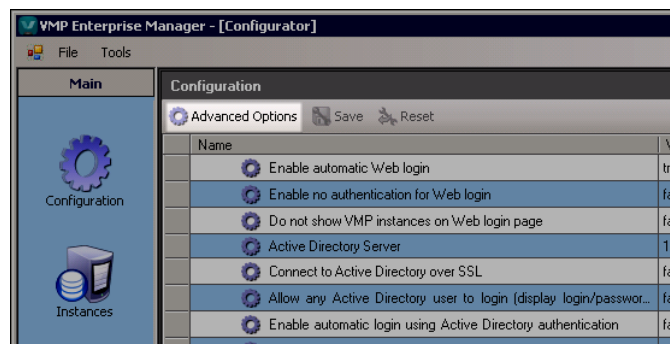
- Click Next, and click Finish.

Configuring WCTP Security

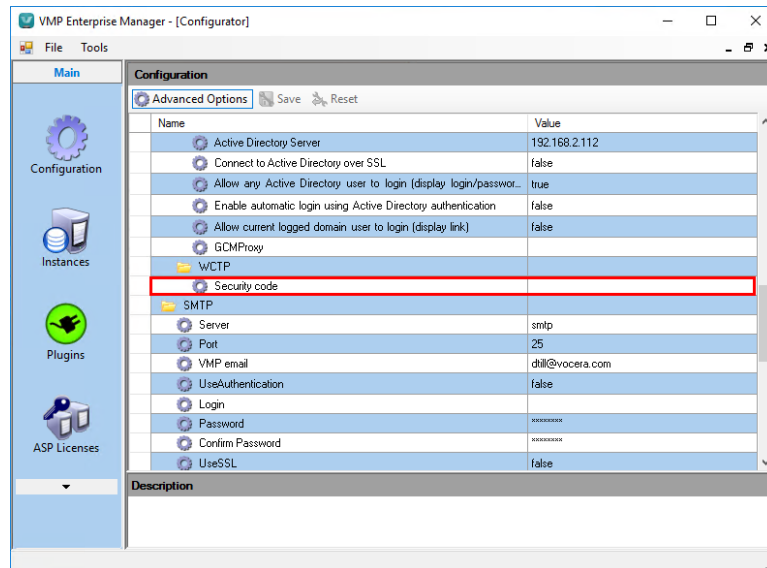
To use the WCTP gateway, you must provide a valid security code. If you do not provide this code, a WCTP request is rejected with a WCTP 402 error.

Use the following steps to provide the valid WCTP security code.

- Start the VMP Enterprise Manager.
- Select Configuration and click Advanced Options.



- Scroll down to WCTP and enter a Security Code.



4. Click Save.
5. Click OK to confirm the saved settings, and click Yes to restart the server.

SOAP Connections

VMP supports inbound SOAP messages from external systems, and forwards these messages to end-users' mobile devices.

SOAP provides considerable flexibility for structuring inbound messages.

For more information on the SOAP interface to VMP, and on the entry points, data classes, and methods that are defined for it, see the *Vocera Messaging Platform API Guide*.

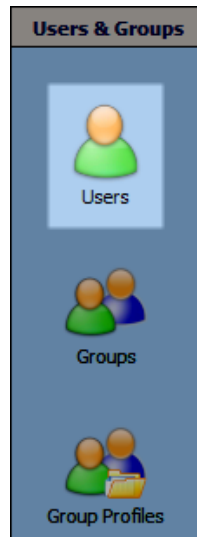


Note: By default, VMP licenses do not include access to the WCTP or SOAP connectors. VMP must be licensed to use the SOAP connector. See [Configuring the VMP License](#) on page 19 for more information.

Configuring VMP to Receive SOAP Messages

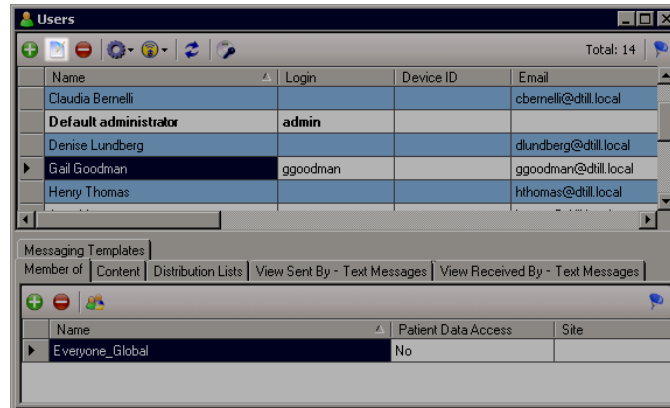
Users or distribution lists that are configured to receive SOAP messages can be set up manually using the VMP Administrator.

1. Start the VMP Administrator.
2. To configure a user to receive SOAP messages:
 - a. Select Users & Groups > Users.



The Users window appears.

- b. Click to highlight the user that is to be configured to receive SOAP messages, and click Edit.



- c. Enter a value in one of the following fields that will match the identifier provided in the SOAP input:
- AD Account (visible only if the VMP Server has been configured to allow any Active Directory user to log in)
 - Pager ID
 - Vocera ID

Edit User

Step 1: End-User Settings

Step 2: Push Technology and Licensing

First Name: [g] [OK]

Middle Name: []

Last Name: Goodman

Title: []

Email: ggoodman@dtill.local

Public ID: []

Pager ID: []

Vocera ID: u-ggoodman

Home Site: Global

Auto Forwarding

Allow Forwarding: Follow System Settings (Yes)

Forward To: [] Remove

Desktop and Web Access

☐ Enable PC Admin Console Access

☒ Enable Web Console Access

Active Directory Authentication

AD Account: DTILL\ggoodman

Vocera credentials

Login: ggoodman

Password: Click here to change...

Confirmation: []

Next > Cancel Help

- d. Click Next, and click Finish.
3. To configure a distribution list to receive SOAP messages:
 - a. Select Messaging > Distribution Lists.
 - b. Click to highlight the distribution list that is to be configured to receive SOAP messages, and click Edit.

Distribution List - Users

Total: 3

Name	Type	Site	Enabled for Texting
Active Directory	Regular		No
Doctors	Regular	Global	Yes
Everyone_Global	Regular	Global	Yes

- c. Enter a value in the Distribution List ID field that will match the identifier provided in the SOAP input.



Note: If the Vocera ID field is available, you can use it to match the identifier provided in the SOAP input.

Edit Distribution List - Users

Name and Type
 Enter a name for the Distribution List (DL) that is being created. Check the 'On-Call Distribution List' checkbox to enable on-call functionality so that only members of the DL who have a status of 'On-Call' or 'Monitor' will receive a Alert sent to DL. The Minimum Users On-Call defines the minimum number of DL members that can be On-Call at any one time.

Name and Type
 Users
 DL Access

Distribution List Name:
 Doctors

Distribution List ID:
 (highlighted with a red rectangle)

Site:
 (dropdown menu)

☐ Enable for Texting

☐ On-Call Distribution List

Minimum Users On-Call: 0

☒ Hidden

Members
☒ Add Users Manually
☐ Create DL based on Active Directory structure

Next > Cancel Help

d. Click Next, Next, and Finish.

Email Monitoring With VMP Messages

Vocera Messaging Platform provides features to integrate user email into the Messaging feature. The server monitors the email box and sends a message to the user when new mail is received.

The following services are supported:

- POP3
- IMAP
- Exchange Web Services (EWS)

The email body is expected to contain an XML document with specific tags used by the VMP Server. Email aliasing and redirection are not necessary, as email messages are sent directly to the monitored mailbox. The XML document contained in the email body defines the recipients for the message. The email header fields are not used to determine the recipients and sender information.

To view an example, see [XML Email Template](#) on page 114.

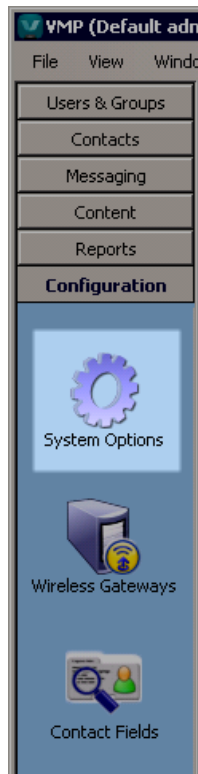
Configuring VMP for Message Email Integration

You can use the VMP Administrator to specify the configuration parameters for sending messages using email.



Note: For email messages, the VMP Server supports Plain Text format only. The email body must be in XML format.

1. Start the VMP Administrator.
2. Select Configuration > System Options.



The System Options dialog box appears.

3. Scroll to Integrations > Email.
4. From the Enable Secure Message Initiation dropdown list, select Yes.

System Options	
User ID	pZeM7xAfAzWL
Shared Key	wjYlrVPx6ySZLoio0...
Email	
Enable Secure Message Initiation	Yes
Secure Message Initiation - Incoming Mail	
Protocol	POP3
Email Scan Interval (in seconds)	30
Initiation Permitted	From VMP users only
Email Username	
Email Password	*****
Confirm Email Password	*****
POP3/IMAP4/EWS Host	
POP3/IMAP4/EWS Port	110
Delete Email Once Processed	Immediately
WCTP	
PollingID 1	
PollingID 2	
PollingID 3	
Description	
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

5. In the Secure Message Initiation - Incoming Mail section, provide the configuration settings that are appropriate for your POP3, IMAP4, or Exchange Web Services deployment. See the *Secure Message Initiation - Incoming Mail* section of the Integrations table in [VMP Administrator Configuration Options](#) on page 245 for a complete description of these options.
6. Scroll back to System and Networking > Email.
7. Set Enable Outgoing Email to Yes. This ensures that delivery and response updates can be sent back to the email initiator.

8. Provide the outgoing email settings that are appropriate for your SMTP deployment. See the *Email* section of the System and Networking table in [VMP Administrator Configuration Options](#) on page 245 for a complete description of these options.

The Email Body Format

Because the email body is in XML Format, email aliasing and redirection are not required, as the XML document contains all of the necessary information.

The following XML tags are supported:

Tag	Description
AlertExternalID:	The ID of the message, as specified by the initiating process or system.
From:	The sender or initiator's name and email address. The value stored in the <i>From</i> field must match the <i>Email</i> and <i>Public ID</i> fields in an existing VMP user definition. See Adding Users Manually on page 117 for more information on the fields that can be specified for a VMP user.
To:	A list of one or more recipient email addresses. The value stored in the <i>From</i> field must match the <i>Public ID</i> field in an existing VMP user definition, or the <i>Distribution List ID</i> field in an existing VMP Distribution List definition. See Adding Users Manually on page 117 for more information on the fields that can be specified for a VMP user, and see Creating a Regular or On-Call Distribution List on page 152 for more information on creating a Distribution List.
Subject:	The message subject.
Message:	The body of the message.
Priority:	The message priority. Must be one of Normal, High, or Urgent.
OverridePersonalAlarmSettings:	Whether the message should force the recipient's device to emit a tone and vibration. Valid options are True and False.
notifyWhenDelivered:	Whether the Delivered status notification should be sent back to the initiator.
notifyWhenRead:	Whether the Read status notification should be sent back to the initiator.
sendResponse:	Whether the initiator should be notified when a recipient sends a response.
notificationEmail:	The email address for status notifications. Overrides the email address specified in the <i>From</i> : tag.
ResponseType:	The response type associated with the message. This is one of the following: <ul style="list-style-type: none"> None: No response is required. Multi: Recipients must select from one or more responses defined in the message.
Responses:	When <i>ResponseType</i> is set to Multi, this is a container tag for the responses defined for the message. Each response is contained in an <i>EmailPagingAlertResponse</i> , which is defined below.

Each *EmailPagingAlertResponse* tag contained in the *Responses* includes the following subtags:

Subtag	Description
RspExternalID:	The third-party ID associated with this response. This ID is returned to the initiating system if the recipient selects this response.

Subtag	Description
Text:	The text that is displayed for this response.

XML Email Template

Here is an example of an XML email template.

```
<?xml version="1.0"?>
<EmailPagingAlert>
  <AlertExternalID>externalID1</AlertExternalID>
  <From>user_sender@company.com</From>
  <To>
    <string>user_recipient@company.com</string>
    <string>dl_recipient@company.com</string>
  </To>
  <!-- Urgent, High, Normal -->
  <Priority>Normal</Priority>
  <OverridePersonalAlarmSettings>true</OverridePersonalAlarmSettings>
  <notifyWhenDelivered>true</notifyWhenDelivered>
  <notifyWhenRead>true</notifyWhenRead>
  <sendResponse>true</sendResponse>
  <notificationEmail>user_sender@company.com</notificationEmail>
  <Subject>Test subject</Subject>
  <Message>Test message</Message>
  <!-- None, Multi -->
  <ResponseType>Multi</ResponseType>
  <Responses>
    <EmailPagingAlertResponse>
      <RspExternalID>extid1</RspExternalID>
      <Text>Response 1</Text>
    </EmailPagingAlertResponse>
    <EmailPagingAlertResponse>
      <RspExternalID>extid2</RspExternalID>
      <Text>Response 2</Text>
    </EmailPagingAlertResponse>
  </Responses>
</EmailPagingAlert>
```

The VMP Administrator

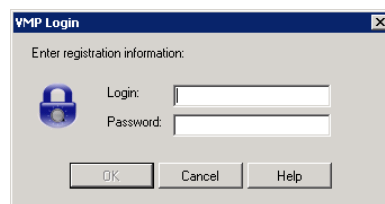
The VMP Administrator enables you to perform all necessary administrative tasks for the VMP Server. It can be installed on the same computer as the VMP Server or on a separate machine.

Logging into the VMP Administrator

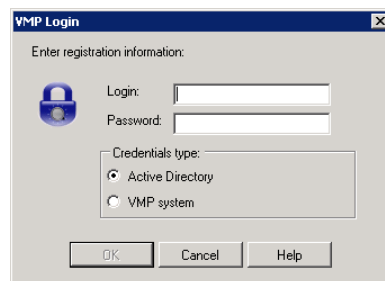
To use the VMP Administrator, you must first log into it.

1. Open the VMP Administrator.
2. Select Start > All Programs > VMP > VMP Administrator.

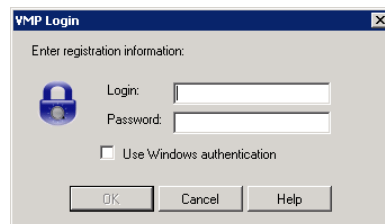
The VMP Login dialog appears. The appearance of this dialog depends on the login options that have been configured. By default, the dialog asks you to type your VMP login name and password:

The image shows a Windows-style dialog box titled "VMP Login". It has a standard Windows icon in the top-left corner. The text "Enter registration information:" is at the top. Below it, there is a blue padlock icon. To the right of the padlock are two text input fields: "Login:" and "Password:". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

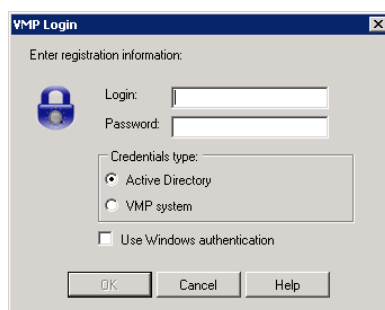
If the Allow any Active Directory user to login configuration option has been set to **true**, radio buttons enable you to specify whether to use Active Directory or VMP credentials to log in:

This image shows the "VMP Login" dialog box with an additional section. Below the "Password:" field, there is a label "Credentials type:" followed by two radio buttons. The first radio button is selected and is labeled "Active Directory". The second radio button is labeled "VMP system". The "OK", "Cancel", and "Help" buttons remain at the bottom.

If the Allow current logged domain user to login option has been set to **true**, a checkbox appears that enables you to use Windows authentication to log in:

This image shows the "VMP Login" dialog box with a checkbox. Below the "Password:" field, there is a checkbox labeled "Use Windows authentication". The "OK", "Cancel", and "Help" buttons are at the bottom.

If both of the above options have been set to **true**, both options are available on the login screen:



See [Configuring VMP for Active Directory](#) on page 37 for more information on configuring the VMP Server for use with Active Directory, and see [VMP Administrator Configuration Options](#) on page 245 for more information on the options shown here.

3. If the **Credentials type** radio buttons are available, select one of the following:

Credentials Type	Description
Active Directory	Select this option to log in using your Active Directory credentials.
VMP system	Select this option to log in using your VMP system credentials if you have been authorized to do so. See Adding Users Manually on page 117 for details on setting the Enable PC Admin Console Access option to authorize user access to the VMP Administrator.

4. Alternatively, if the **Use Windows authentication** checkbox is available, select it to use your Windows authentication credentials to log into the VMP Server.
5. If you are not using Windows authentication, type the **Login** and **Password**, and click **OK**.

If you are the system administrator and are logging into the VMP Administrator for the first time:

- If the **Credentials type** radio buttons are available, select **VMP system**.
- In the **Login** field, type **admin**.
- In the **Password** field, type the administrative password that you supplied in the **Security Options** dialog box during installation. See [Installing the VMP Server](#) on page 13 for more details.



Note: To exit the VMP Administrator, select **Exit** from the **File** menu.

The VMP Administrator Modules

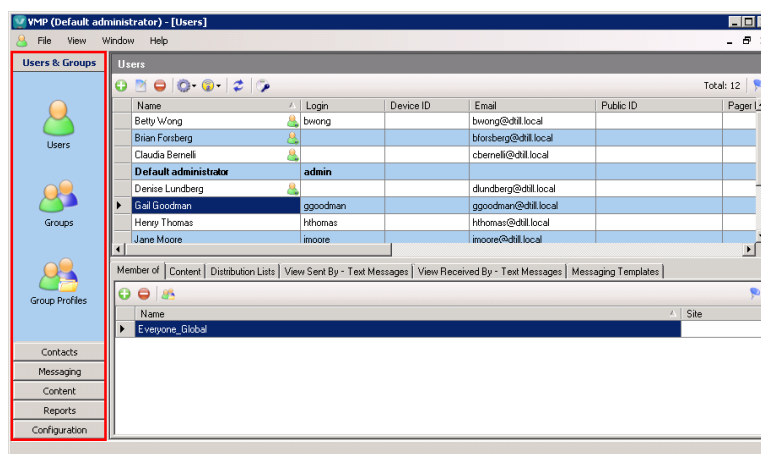
The VMP Administrator is organized into modules, each of which performs a set of common administrative tasks.

The following modules are defined:

- Users & Groups
- Contacts
- Messaging
- Content
- Reports
- Configuration

If you are not the administrator and some or all of these modules are not visible to you, your administrator has not granted the user rights that you need to view them. See [Editing User Rights](#) on page 123 for more information on granting user rights.

To access a module, click its name in the left pane of the VMP Administrator window:



You can also access a module or its components from the View menu.



Note: If multiple windows are being displayed in the VMP Administrator, you can use the Window menu to control the window layout. Select one of Cascade, Tile Horizontally, or Tile Vertically to display all windows, or select a window to view. Select Close to close the window that you are viewing.

Users and Groups

The Users & Groups module provides features to import, create, and manage VMP users. This module also allows you to use groups to create user sets and Distribution Lists to manage access permissions and on-call scheduling.

Users can be entered and updated manually, or VMP can synchronize with contact lists in other corporate systems.



Note: Some of the features found in the Users & Groups module are covered in the following sections:

- [About Importing and Synchronizing](#) on page 48, which describes how to import users and contacts from a Vocera Voice Server, an Active Directory server, and a SQL server, and how to import from Excel and CSV files.
- [Sending Installation Information to User Devices](#) on page 74, which describes how to send installation and registration instructions to a client device.

About Adding and Deleting Users Manually

If you want to add a user that is not included in your remote resource, you can add the user manually. You can also manually delete users from the system.

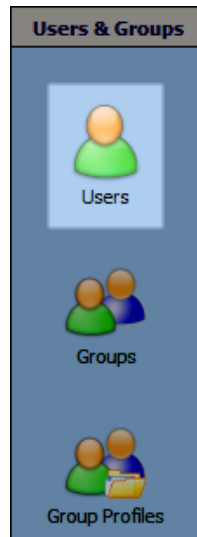


Tip: When editing imported users, do not edit fields that synchronize with the imported source. These changes should be made at the source to avoid overwriting the changes when the source synchronizes with the VMP Server. If the email address of a contact is changed on the VMP Server, or the Public ID of the contact is changed if no email address is provided, the contact will not synchronize with the source.

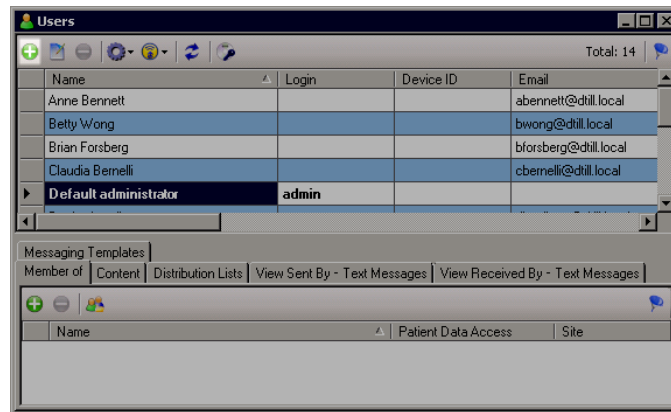
Adding Users Manually

If you want to add a user that is not included in your remote resource, you can add the user manually.

1. From the VMP Administrator, select Users & Groups > Users.



2. In the toolbar in the Users pane, click Add.



The End-User Settings window appears.

New User

Step 1: End-User Settings

Step 1: End-User Settings
Step 2: Push Technology and Licensing

First Name:

Middle Name:

Last Name:

Title:

Email:

Public ID:

Pager ID:

Vocera ID:

Home Site:

VST ID:

Auto Forwarding

Allow Forwarding:

Forward To:

Profile:

Desktop and Web Access

☐ Enable PC Admin Console Access

☒ Enable Web Console Access

Vocera credentials

Login:

Password:

Confirmation:

3. Enter the following end-user settings.

Table 23: End-user settings

Field	Description
First Name	The first name of the user.
Middle Name	The middle name of the user (optional).
Last Name	The last name of the user.
Title	The job title for the user.
Email	The email address for the user.
Public ID	The user's public ID. This optional field can be used to identify the recipient in APIs that are supported in VMP.
Pager ID	The user's pager ID. This optional field is populated when the VMP Client Gateway API is implemented.
Vocera ID	The user's Vocera ID. This optional field is populated when the VMP Client Gateway API is implemented.
Home Site	The site to which the new user is to belong. Sites are available if they have been created on the Vocera Voice Server with which the VMP Server has been integrated. See Vocera Voice Server Integration on page 30 for more information on integrating with the Vocera Voice Server.
VST ID	If a user has been imported from a Vocera Secure Texting cloud server, this field contains the StaffID value that was assigned when the user was created in VST.
Allow Forwarding	Use this dropdown list to allow forwarding of messages from this user to another user. Select <i>Follow System Settings</i> (the current system setting is shown in brackets), <i>Yes</i> , or <i>No</i> .

Field	Description
Forward To	When <i>Allow Forwarding</i> is enabled, this specifies the user to which messages are being forwarded. This is set in the Vocera Collaboration Suite application only. To remove forwarding if it has been set up, click <i>Remove</i> .
Profile	Select from this dropdown list to associate the user with a group profile. See Group Profiles on page 135 for more information on group profiles.
Enable PC Admin Console Access	Select this checkbox to allow the user to access the VMP Administrator.
Enable Web Console Access	Select this checkbox to allow the user to access the VMP Web Console. Activating this field requires you to enter authentication credentials for the user.
AD Account	If the new user has an Active Directory account, enter the account name in the <i>AD Account</i> field. This option appears if VMP Administrator access with Active Directory credentials is configured during installation.
Vocera credentials	To provide Vocera credentials for the new user, enter the VMP Administrator login in the <i>Login</i> field, enter the password in the <i>Password</i> field, and re-enter the password in the <i>Confirmation</i> field.

- Click **Next** to display the Push Technology and Licensing window.

The screenshot shows the 'Edit User' window with the title bar 'Edit User' and a close button. The main content area is titled 'Step 2: Push Technology and Licensing'. On the left, there is a sidebar with 'Step 1: End-User Settings' and 'Step 2: Push Technology and Licensing'. The main area contains the following sections:

- Mobile Device Access:**
 - ☒ **Enable**
 - Device type: Vocera Smartphone Client (dropdown)
 - Registration Key: (text field) ☐ **Generate key**
 - Device PIN: (text field)
 - Enforce App PIN: Follow System Settings (Shared) (dropdown)
- VMP Applications On Device:**
 - Application Name (dropdown)
 - ☒ **Alert**
 - ☐ Alert(SMS)
 - ☐ Alert(SNPP/WCTP/TAP)
 - ☐ **Chat**
 - ☐ Contacts
 - ☐ Content

At the bottom, there are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'.

- To enable mobile device access, select the **Enable** checkbox, and select the device type from the **Device type** dropdown list.
- To register the user, type the registration information in the fields provided.



Note: For details on how to generate a registration key and email this registration information to the user, see [Sending Installation Information to User Devices](#) on page 74.

- From the **Enforce App PIN** dropdown list, select one of the following:

Follow System Settings	Use the setting defined in the Enforce App PIN configuration option, which is set in the VMP Administrator. This is the default. This option displays the current system setting, which is one of Off, On, or Shared.
Enforce PIN	Enforce the use of an application-level PIN for this user.
Do Not Enforce PIN	Do not require this user to provide an application-level PIN, even if a PIN is normally required.

8. In the VMP Applications On Device pane, select the VMP applications to which the user is to be granted access. Access can be granted to an application only if at least one unused license is available.



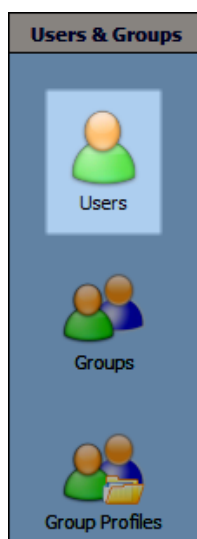
Note: For Vocera Collaboration Suite users, ensure that the Alert, Chat, and Contacts applications are selected. Select Content if you want to provide documents, image files, or other content to these users.

9. Click Finish to finish creating the new user.

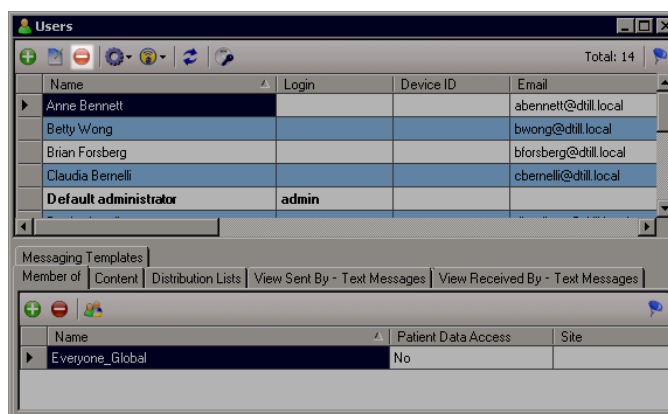
Deleting a User

You can manually delete any user, and can optionally wipe all data stored in the user's smartphone application.

1. From the VMP Administrator, select Users & Groups > Users.



2. In the Users pane, click the name of the user to be deleted.
3. In the toolbar, click Delete.

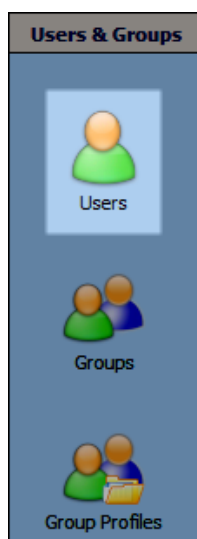


4. In the confirmation dialog box that appears, select the **Wipe data on smartphone** checkbox (if it is enabled) to wipe all data stored in the smartphone application.
5. Click **Yes** to confirm user deletion.

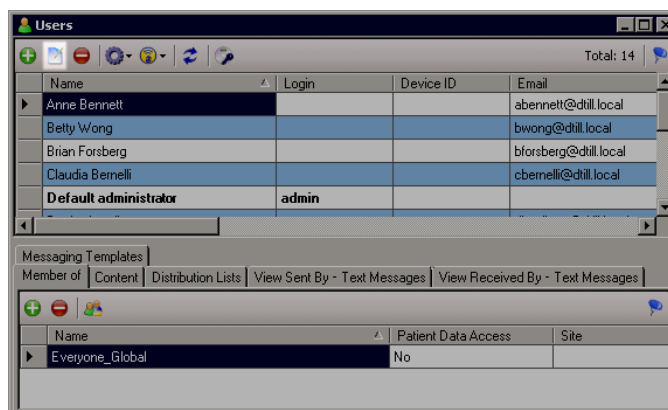
Editing User Information

For any user, you can edit the information, device registration, and list of applications to which access has been granted.

1. From the VMP Administrator, select **Users & Groups > Users**.



2. In the **Users** pane, click the name of the user whose information is to be edited.
3. In the toolbar, click **Edit**.



The End-User Settings window appears.

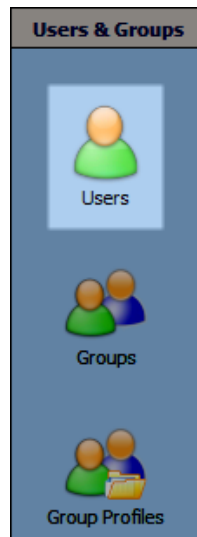
4. Edit the user fields as needed. For more information on user fields, see [Adding Users Manually](#) on page 117.

Editing User Rights

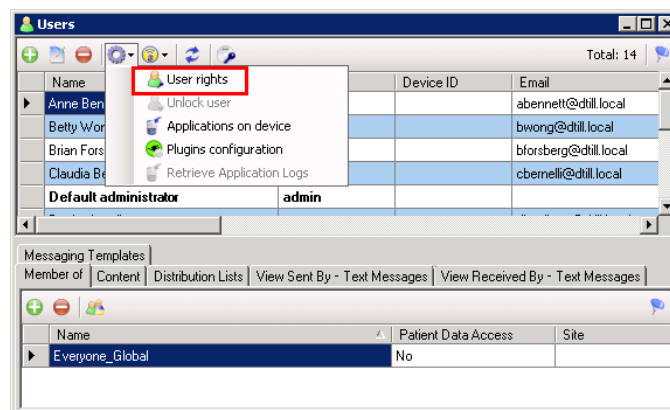
In the VMP Administrator, you can specify the rights that are to be granted to any user on the system.

You can also assign a user to one or more Right Groups. Each Right Group grants a specific set of user rights.

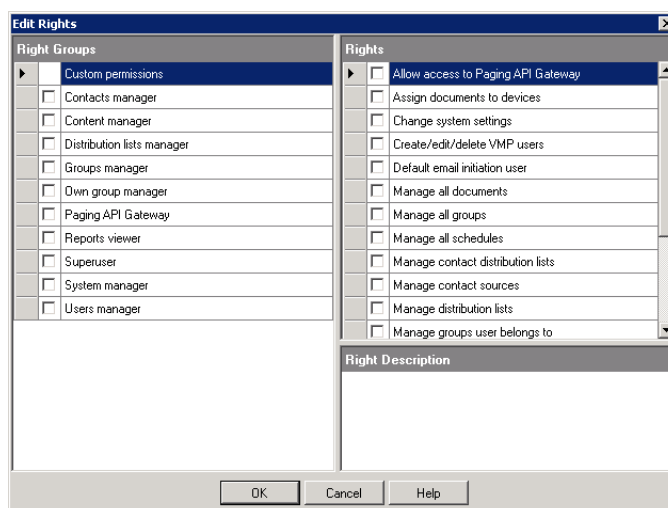
1. From the VMP Administrator, select **Users & Groups > Users**.



2. In the Users pane, click the name of the user for which user rights are to be edited.
3. In the toolbar, from the User preferences dropdown list, select **User rights**.



The Edit Rights dialog box appears.



4. In the Right Groups pane, click a Right Group. The rights associated with the Right Group appear in the Rights pane. To grant these rights to the user, select the checkbox next to the Right Group. Repeat this for other Right Groups as needed.

See [Right Groups](#) on page 125 for a list of the available right groups.

5. To grant custom permissions without selecting a Right Group, click Custom permissions to display a list of rights in the Rights pane. Select the checkboxes of the rights that you want to grant. See [User Rights](#) on page 124 to view a list of the available rights.



Note: Rights that have been granted by assigning a user to a Right Group are already selected, and cannot be changed in this way.

6. Click OK to finish granting rights to the selected user.

User Rights

You can grant rights to VMP Administrator users to enable access to the server's capabilities.

User Right	Description
Allow access to Paging API Gateway	Allow use of the SOAP API interface. For more information on this interface, see the <i>Vocera Messaging Platform API Guide</i> .
Assign documents to devices	Deprecated - no longer in use.
Change system settings	Enable access to the Configuration settings in the VMP Administrator and the Group Profiles screen in the Users & Groups section.
Create/edit/delete VMP users	Enable access to the Users screen in the Users & Groups section of the VMP Administrator. Enabling this user right does not grant permission to view the View Sent By - Text Messages and View Received By - Text Messages tabs in the Users screen. To grant permission to view these tabs, you must grant the Manage who views VMP pager alerts user right.
Default email initiation user	Deprecated - no longer in use.
Manage all documents	Enable permission to import and share content.
Manage all groups	Enable access to the Groups screen in the Users & Groups section of the VMP Administrator.
Manage all schedules	Grant permission to create and manage schedules that anyone has created in the VMP Web Console. For more information, see Granting Users Scheduling Permissions on page 224.
Manage contact distribution lists	Enable edit access to the Distribution Lists screen in the Contacts section of the VMP Administrator. Without this permission, users can view the Distribution Lists screen, but cannot add, update, or change contact distribution lists.

User Right	Description
Manage contact sources	Enable access to the Contact Sources screen in the Contacts section of the VMP Administrator.
Manage distribution lists	Enable access to the Distribution Lists screen in the Messaging section of the VMP Administrator.
Manage groups user belongs to	Deprecated - no longer in use.
Manage schedules	Grant permission to create and manage schedules that you have created in the VMP Web Console. For more information, see Granting Users Scheduling Permissions on page 224.
Manage who views VMP text messages	In the Users screen, grant access to view the View Sent By - Text Messages and View Received By - Text Messages tabs. To grant this user right, you must also grant the Create/edit/delete VMP users user right.
View all distribution lists	Deprecated - no longer in use.
View all messaging templates	Grant permission to edit existing messaging templates. Without this permission, users can view and create templates, but can only edit templates that they have created.
View all pager alerts in the report	Deprecated - no longer in use.
View all reports	Enable permission to access the Reports section to open and view reports.
Patient Data Access	Enable permission to access Engage patient data. This right is not editable in this view. See Integrating with the Engage Patient Context Adapter on page 39 for information on how to integrate VMP with the Engage Patient Context Adapter and how to grant patient data access to a user.

Right Groups

You can assign VMP Administrator users to right groups. Each right group grants one or more rights to its members.



Note: Some of the rights listed here are now deprecated because they are no longer in use. See [User Rights](#) on page 124 for more details. A right group is marked as deprecated if all of its rights are deprecated.

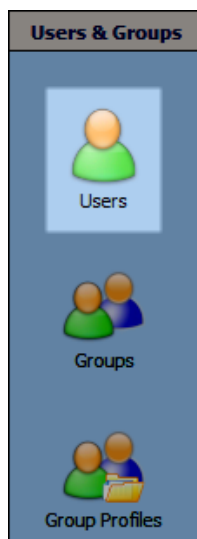
Right Group	Rights included in group
Contacts manager	Manage contact distribution lists Manage contact sources
Content manager	Assign documents to devices Manage all documents
Distribution lists manager	Manage distribution lists Manage schedules
Groups manager	Manage all groups
Own group manager	Assign documents to devices Manage groups user belongs to
Paging API Gateway	Allow access to Paging API Gateway
Reports viewer	View all reports

Right Group	Rights included in group
Superuser	Allow access to Paging API Gateway Assign documents to devices Change system settings Create/edit/delete VMP users Manage all documents Manage all groups Manage all schedules Manage contact distribution lists Manage contact sources Manage distribution lists Manage groups user belongs to Manage schedules Manage who views VMP text messages View all distribution lists View all messaging templates View all pager alerts in the report View all reports
System manager	Change system settings
Users manager	Create/edit/delete VMP users Manage all groups Manage who views VMP text messages

Unlocking a User

If a user has been inactive for a specified number of days, the user is placed in a Locked state, and cannot access the server. You can unlock any user that has been Locked.

1. From the VMP Administrator, select **Users & Groups > Users**.



2. In the Users pane, click the name of the user to be unlocked.
3. In the toolbar, from the **User preferences** dropdown list, select **Unlock user**. The selected user is unlocked.

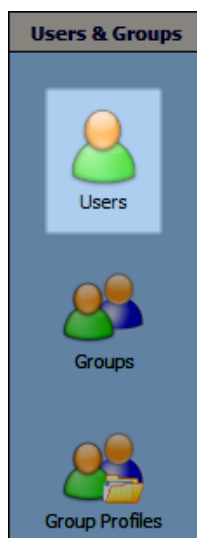


Note: The number of days of inactivity before a user is placed in a Locked state is specified in the **Configuration > System Options** section of the VMP Administrator.

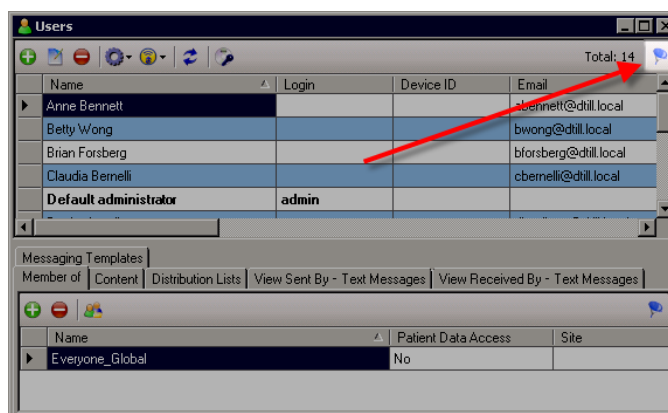
Filtering the User Display

You can filter the list of users to make it easier to find a particular user.

1. From the VMP Administrator, select **Users & Groups > Users**.



2. Click Filter.



The Filter Users popup appears.

First Name:

Middle Name:

Last Name:

Title:

Email:

Login:

Device ID:

Device type:

Wireless gateway:

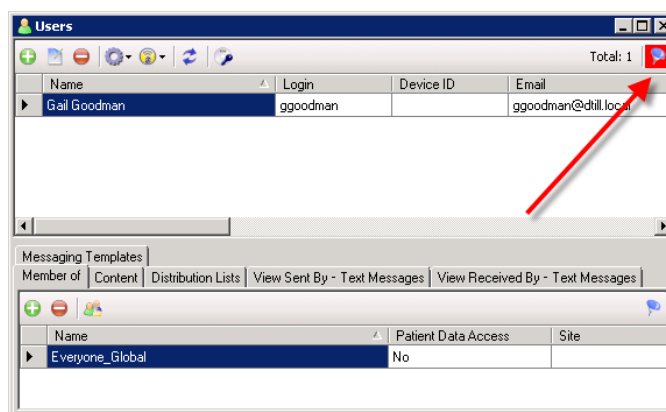
Member of:

Name	Site
Everyone_Global	No

Select Remove groups

3. To improve filtering, enter a search string in any or all of the fields provided, and select an item from any or all of the dropdown lists provided.
4. To filter by group, click **Select** and add one or groups to the filter list. To remove a group from the list, highlight it and click **Remove groups**.
5. Click anywhere outside the popup to close it.

When you enter a search string in a text field, select an element from a dropdown list, or specify a group, the Users list automatically updates to use the filtering that you have specified, and the Filter icon changes color.



Right-click this icon to reset filtering.

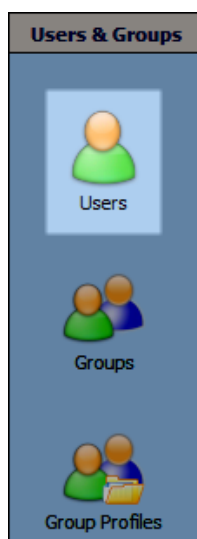
Retrieving Application Logs

From the VMP Administrator, you can retrieve application logs for any VCS user for which a device ID has been specified. This enables you to respond quickly if a problem is detected.



Note: To use this capability, your devices must be using version 3.2 or later of VCS.

1. From the VMP Administrator, select Users & Groups > Users.



2. In the Users pane, click the name of the user for which you want to retrieve the application logs.
3. In the toolbar, from the User preferences dropdown list, select Retrieve Application Logs. The Retrieve Application Logs dialog box appears.
The Retrieve Application Logs option is available only when a Device ID has been specified for the user.
4. In the Notification email address field, optionally type the email address to which to send a notification that logs are available.
5. Click OK to upload the client logs to the VMP Server. These logs are stored in the WIC\Logs subfolder of the folder in which you have installed VMP.



Important: Logs are retrieved without notifying the user. It is your responsibility to create and implement suitable policies to ensure that your use of this capability does not violate applicable laws. For example, you may need to obtain a waiver of privacy rights from employees who use Vocera Collaboration Suite as part of their employment.


Groups

You can use groups to organize users who have similar roles. From groups, you can manage access permissions and on-call scheduling.

From the Users & Groups module, you can:

- Create, rename, and delete groups
- Add users to a group and remove users from a group
- Indicate what items are to be made accessible to the group

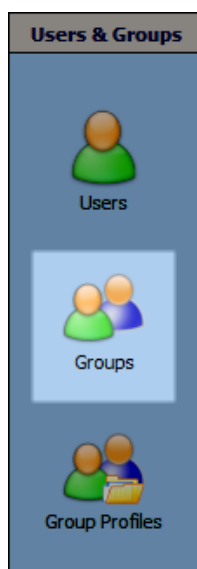


Note: If you have defined a large number of groups, you can use a filter to limit the groups that are displayed. To filter the list of groups, click Filter  and type the filter to use. The Filter icon changes color. Right-click this icon to reset filtering.

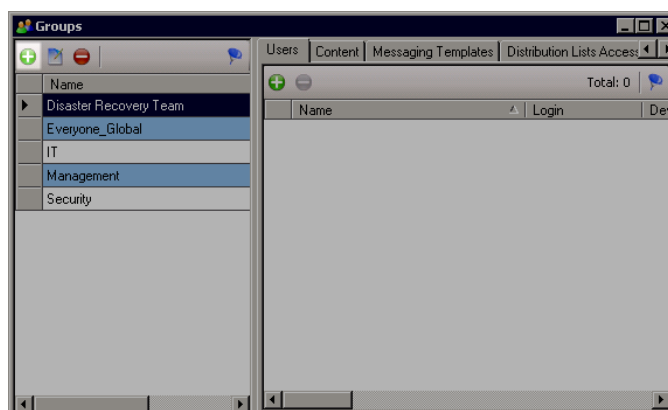
Creating a New Group

From the Users & Groups module, you can create a new group.

1. From the VMP Administrator, select Users & Groups > Groups.



2. In the toolbar in the Groups pane, click Add.

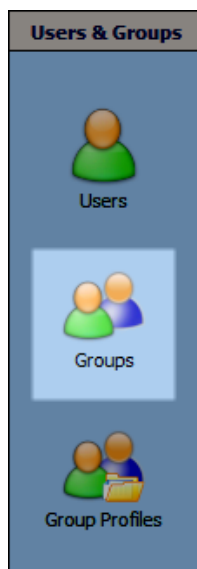


3. In the New Group dialog box, enter the name of the new group and click OK.

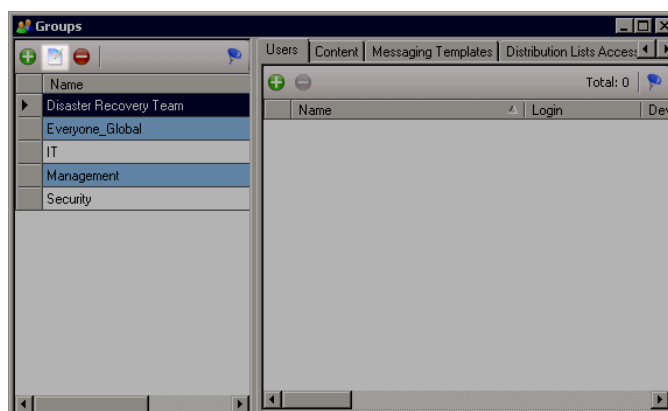
Changing a Group Name

You can change the name of any group that you have created.

1. From the VMP Administrator, select Users & Groups > Groups.



2. In the toolbar in the Groups pane, click Edit.

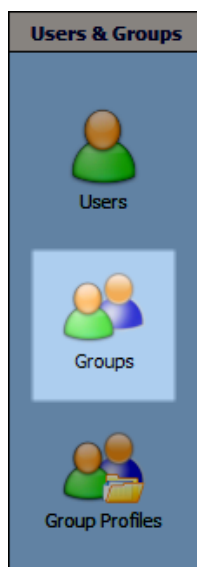


3. In the Edit Group dialog box, enter the new name of the group and click OK.

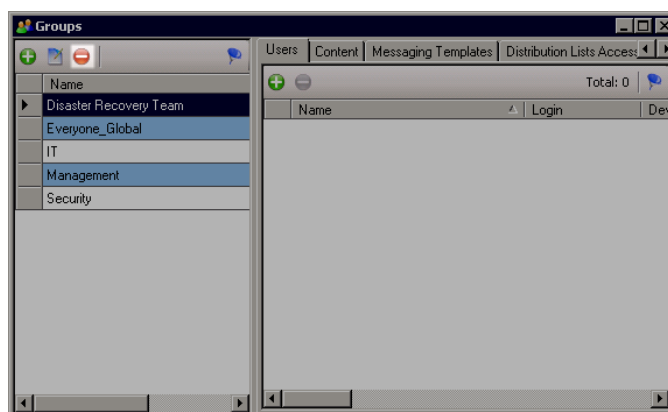
Deleting a Group

From the Users & Groups module, you can delete any existing group.

1. From the VMP Administrator, select Users & Groups > Groups.



2. In the toolbar in the Groups pane, click Delete.

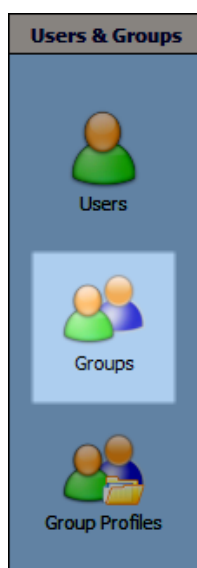


3. When asked to confirm whether you want to delete the group, click Yes.

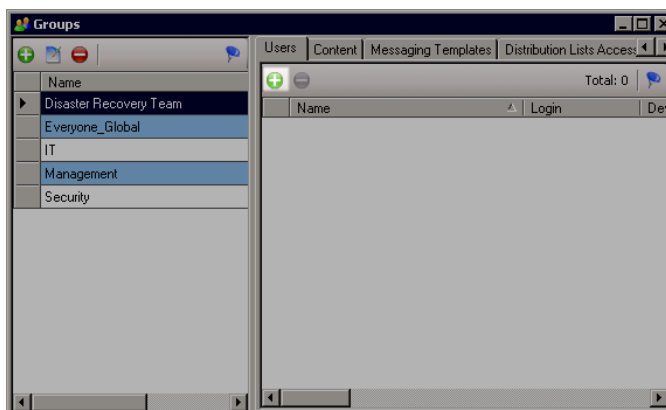
Adding Users to a Group

From the Users & Groups module, you can add users to any existing group.

1. From the VMP Administrator, select Users & Groups > Groups.

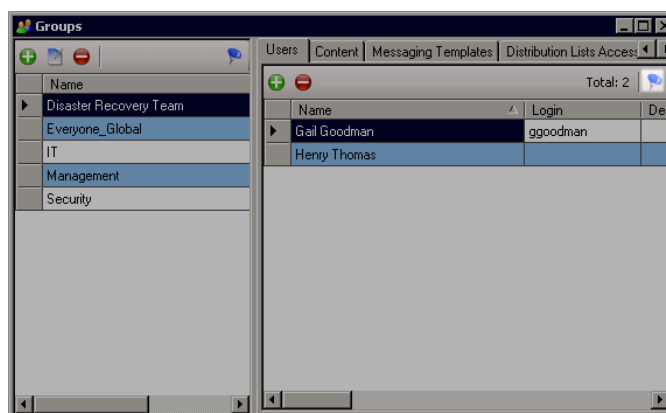


2. In the Groups pane, highlight the group to which you want to add users.
3. In the pane at the right, click the **Users** tab and then click **Add**.

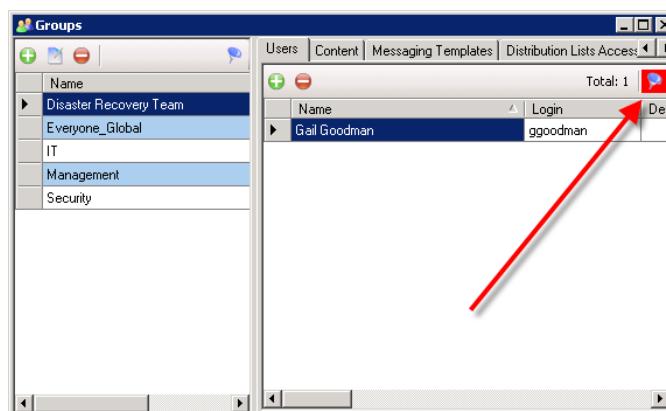


4. In the Select Users dialog box, click to highlight the users to be added and click **OK**.

To filter the list of users in a group or in the Select Users dialog box, click **Filter** and enter the filtering criteria to use.



The Filter icon changes color.

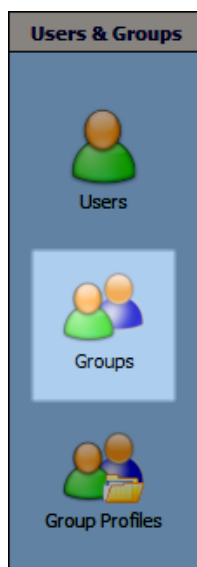


To reset filtering, right-click **Filter**.

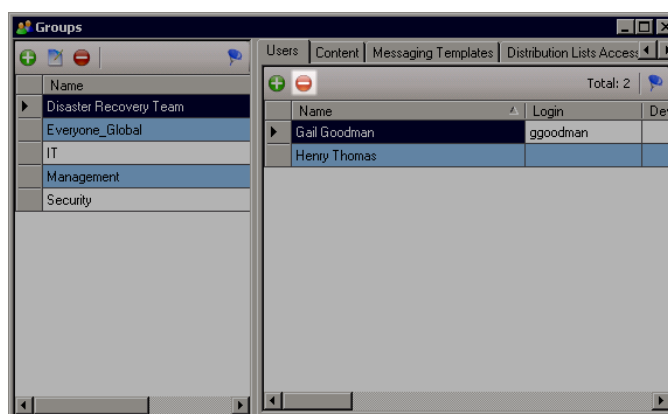
Removing Users from a Group

If a user is no longer required to be in a particular group, you can remove the user from the group.

1. From the VMP Administrator, select **Users & Groups > Groups**.



2. In the Groups pane, highlight the group from which you want to delete users.
3. In the pane at the right, click the Users tab.
4. Highlight the users that you want to delete.
5. Click Delete.

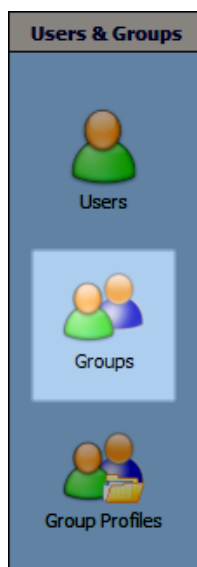


6. When asked to confirm whether you want to delete the users from the group, click Yes.

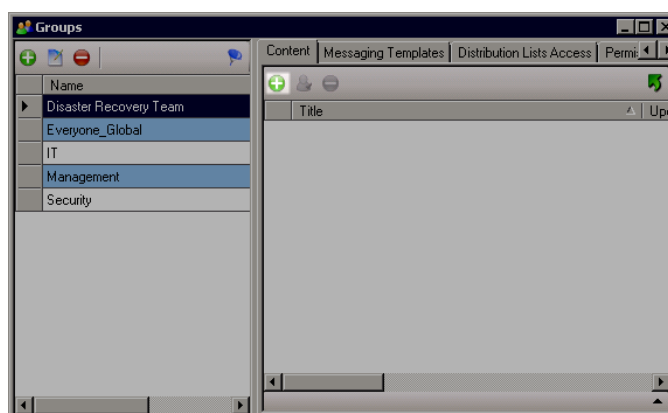
Granting Group Access

You can specify that items such as content, Messaging Templates, and Distribution Lists are to be made accessible to a group.

1. From the VMP Administrator, select Users & Groups > Groups.

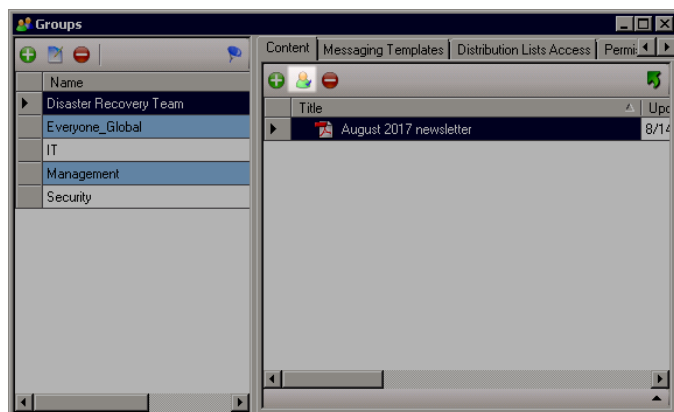


2. In the Groups pane, highlight the group with which you want to associate items.
3. In the pane at the right, click the tab corresponding to the item that you want to make accessible. For example, click **Content** to make content accessible to the group.
4. Click **Add**.

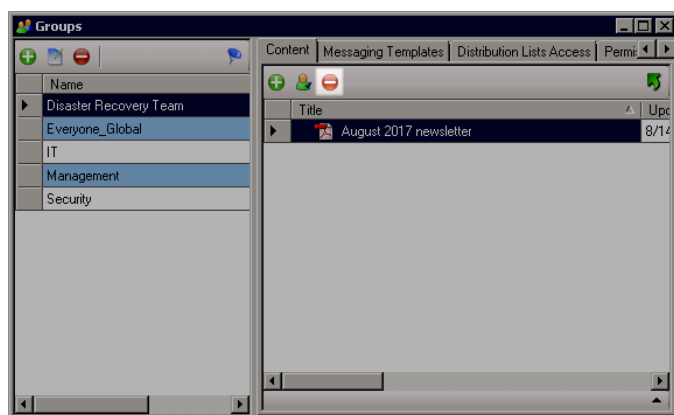


5. From the list of available items, highlight the item to be made accessible.
6. To grant additional permissions, click any or all of the following checkboxes:
 - Allow update
 - Allow delete
 - Allow manage access
 - Visible on device by default
7. Click **OK**.

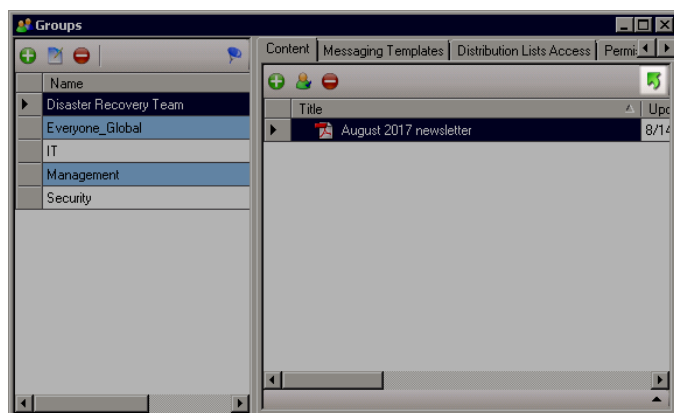
To change the permissions for any item that has been made accessible, highlight the item, click **Manage access**, and click any or all of the permissions checkboxes.



To make an item inaccessible, highlight the item, click Remove, and click Yes to confirm that you want to remove access to the item.



To refresh the list of available content in the Content tab, click Refresh.



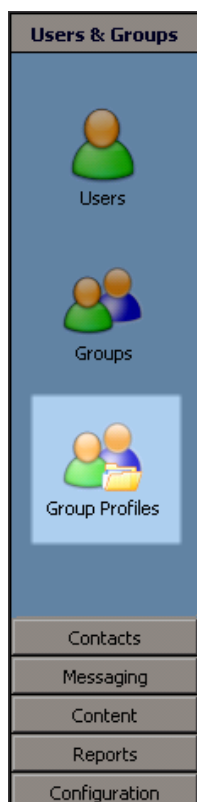
Group Profiles

You can create group profiles for groups that share the same set of fields and permissions. Users that are assigned a group profile become members of all groups belonging to the group profile.

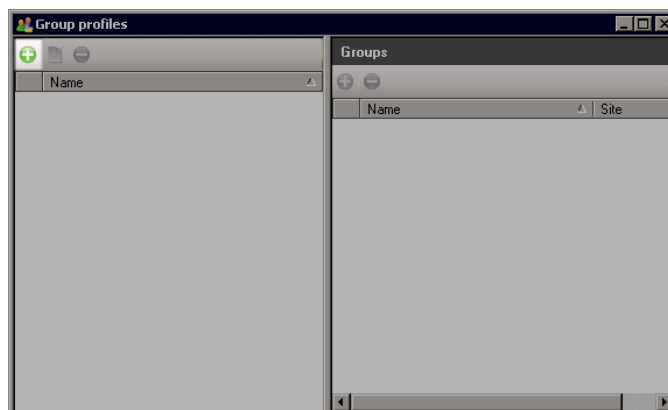
Creating Group Profiles

From the Users & Groups module, you can create a group profile for groups that have the same fields and permissions.

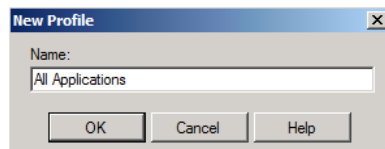
1. From the VMP Administrator, select Users & Groups > Group Profiles.



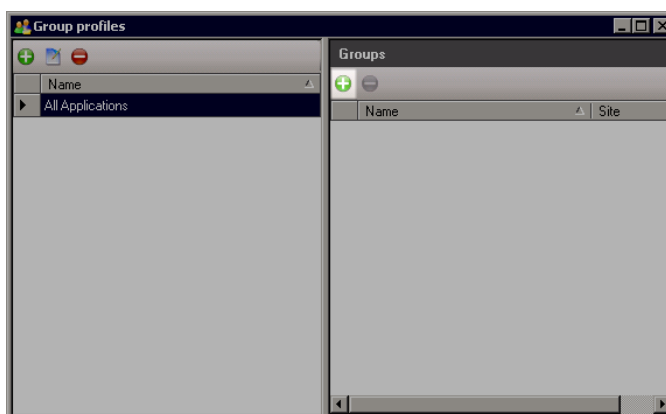
2. Select New.



3. Name the profile, and click OK.



4. With the profile selected under Group profiles, click New.



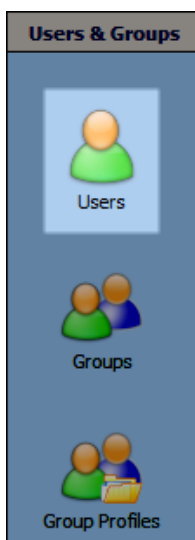
Select the groups to include with the profile.

- Click OK to close the dialog box.

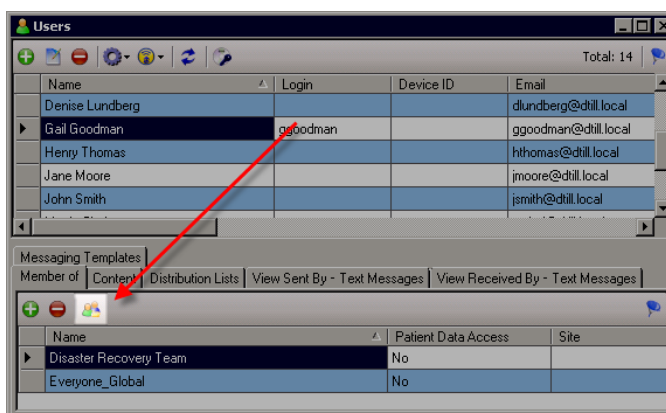
Assigning Group Profiles

From the Users & Groups module, you can assign a group profile to a user. This makes the user a member of all groups in the group profile.

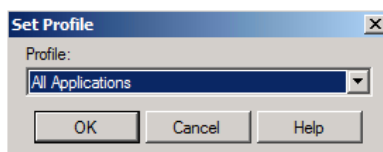
- From the VMP Administrator, select Users & Groups > Users.



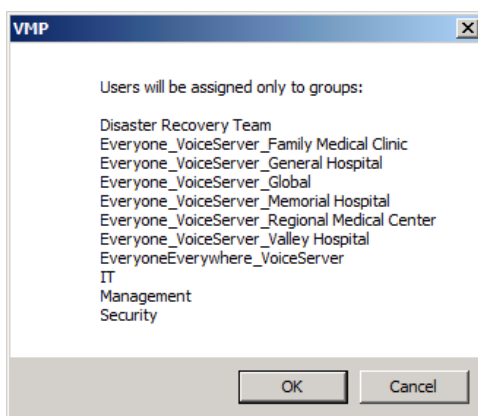
- Click to highlight a user.
- From the Member of tab, select Set Profile.



- Use the dropdown list to select the profile, and click OK to close the dialog.



- Click OK to confirm the assigned groups.



Contacts

The Contacts module enables you to import contact information for people and places that are not VMP users, such as local businesses.



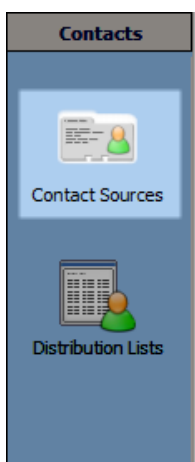
Note: Some of the features found in the Users & Groups module are covered in [About Importing and Synchronizing](#) on page 48, which describes how to import contacts from a source, including from a Vocera Voice Server global address book.

Manually Adding a New Contact

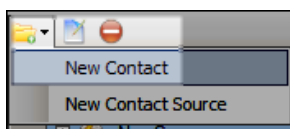
You can use the VMP Administrator to add a new contact manually.

You must already have at least one contact source available in the Contact Sources view.

- Select the Contacts module, and select Contact Sources.

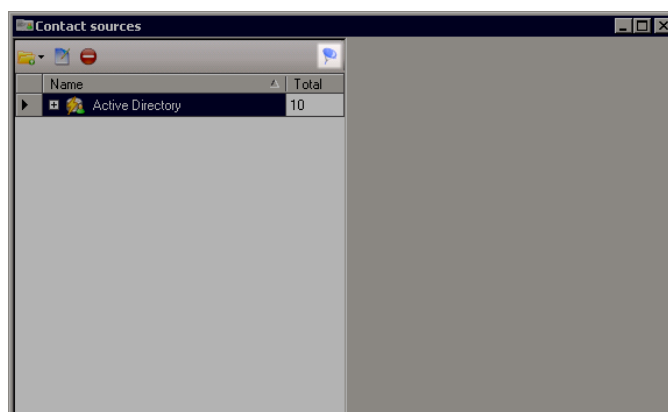


- Click to highlight the contact source that is to contain the new contact.
- Select New and choose New Contact.

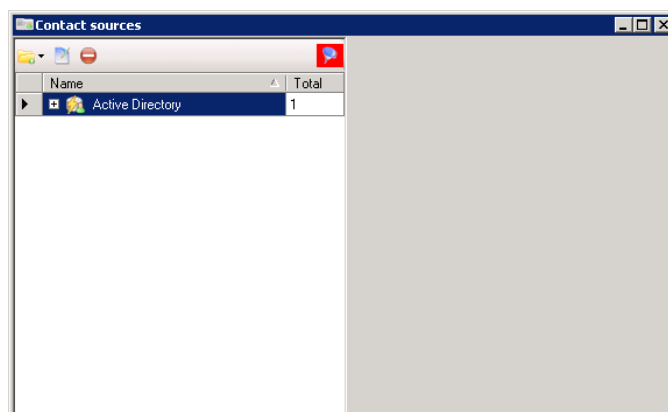


4. Enter the contact details in the New Contact dialog, and click OK.

To filter the list of contact sources, click Filter and select the filter criteria to use.



The Filter icon changes color.

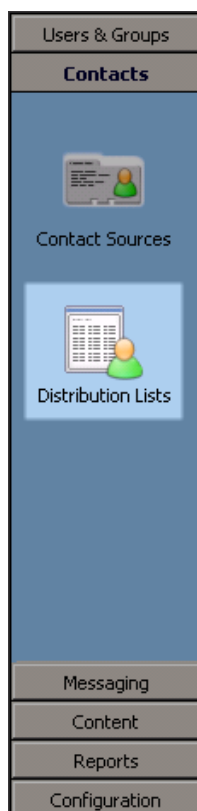



To reset filtering, right-click Filter.

Creating a Contacts Distribution List

Contacts Distribution Lists enable you to organize your contacts for quicker access. You can create a Contacts Distribution List from the Contacts module.

1. Select the **Contacts** module, and select **Distribution Lists**.



2. Select New  from the Distribution List - Contacts view.
3. In the Distribution List name field, enter the name of the new Contacts Distribution List.
4. If sites have been defined, use the Site dropdown list to select the site for this Contacts Distribution List.



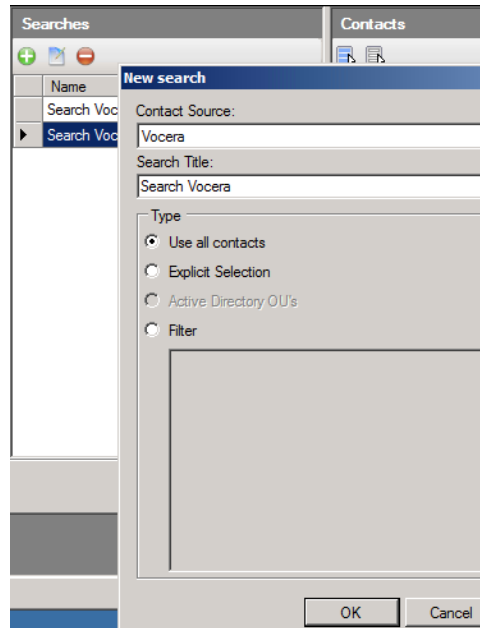
Note: Sites are available if they have been created on the Vocera Voice Server with which the VMP Server has been integrated. See [Vocera Voice Server Integration](#) on page 30 for more information on integrating with the Vocera Voice Server.

5. Select the Hidden checkbox if the Contacts Distribution List is to remain hidden. The contacts that are members of this list remain accessible.
6. In the Distribution List Fields pane, select the fields to display on the client.



Tip: Click Select All  to add all available fields.

7. Click Next.
8. Select the Contact Source in Searches.



9. Select from the following options:

Table 24: Contact source options

Option	Description
Use all contacts	Automatically add all source contacts to the list.
Explicit Selection	Manually choose the source contacts for the list.
Active Directory OU's	If the source is imported from Active Directory, you can choose to add Organization Units.
Filter	Filter for contact to add based on contact fields.



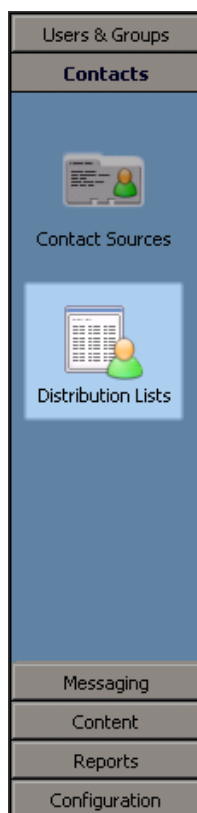
Tip: Filter for contacts with crucial fields (mobile phone, email address, etc.) to ensure you are adding only contacts with these fields populated.

10. Click Next to display the Group Assignment pane.
11. Choose the users and groups who have access to the Distribution List and click Finish.

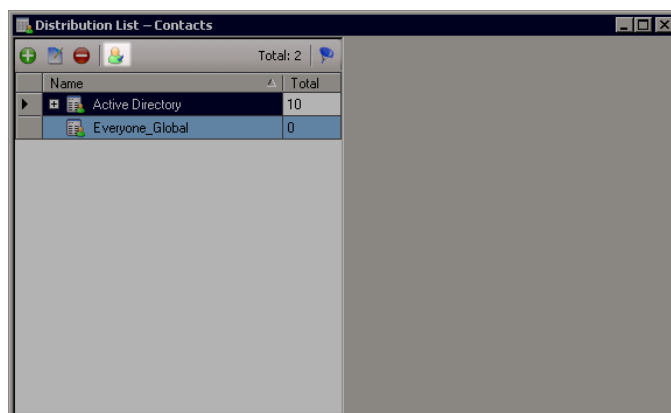
Managing Contacts Distribution List Access

You can control which users and groups can view a Contacts Distribution List.

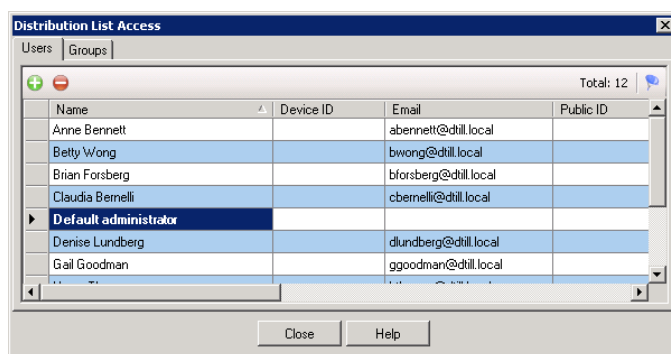
1. Select the Contacts module, and select Distribution Lists.



2. Select a list and click Manage Access.

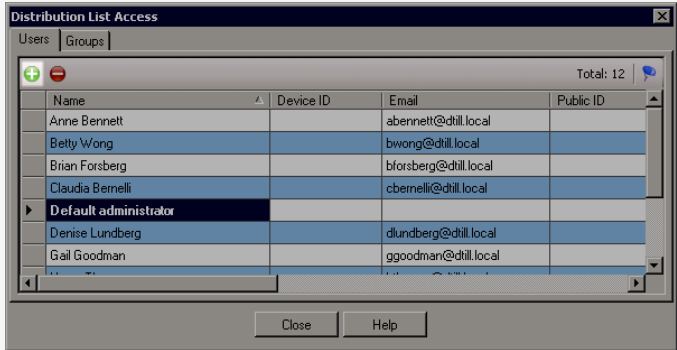
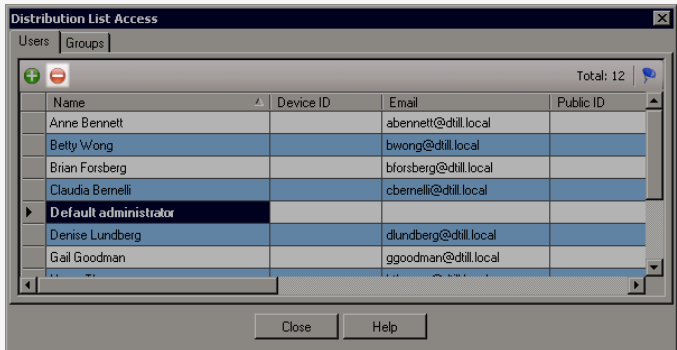


The Distribution List Access dialog box appears.



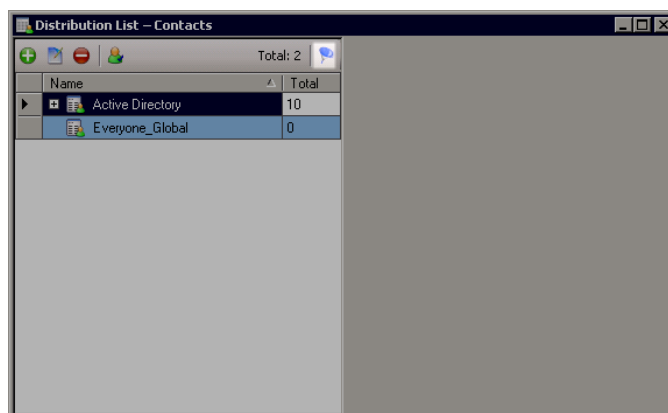
3. The Distribution List Access dialog box allows you to perform the following tasks:

Table 25: Distribution List access task options

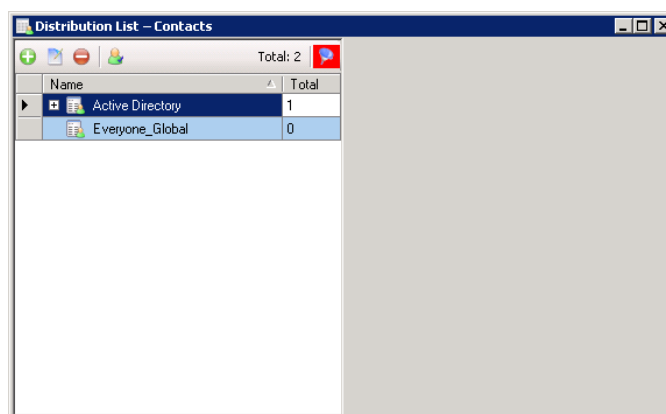
Task	Description
Add User	Click the Users tab, and click Add to select users who can access the list. 
Add Group	Click the Groups tab, and click Add to select groups who can access the list.
Delete User	Click the Users tab, select the user, and click Remove to revoke access to the list. 
Delete Group	Click the Groups tab, select the group, and click Remove to revoke access to the list.

4. Click **Close** to save the access changes.

To filter the list of Contact Distribution Lists, click **Filter** and enter the filtering criteria to use.



The Filter icon changes color.



To reset filtering, right-click Filter.

Messaging

The Messaging module in the VMP Administrator enables you to configure the messaging environment in the VMP Web Console and the Vocera Collaboration Suite app.

In the Messaging module, you can:

- Create Message Templates that enable users to quickly create and send commonly used or urgent messages.
- Create Distribution Lists that enable users to send a message to multiple users simultaneously.

About Messaging Templates

Messaging Templates enable users to quickly create frequently sent or important messages. For example, you can create a Code Blue template to ensure that emergency notifications are sent out immediately.

When you create a Messaging Template, you can specify:

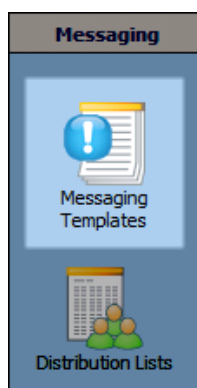
- Which users or groups are to be given permission to access the template.
- The default list of recipients for any message sent using this template.

The list of recipients can contain users, Distribution Lists, or both.

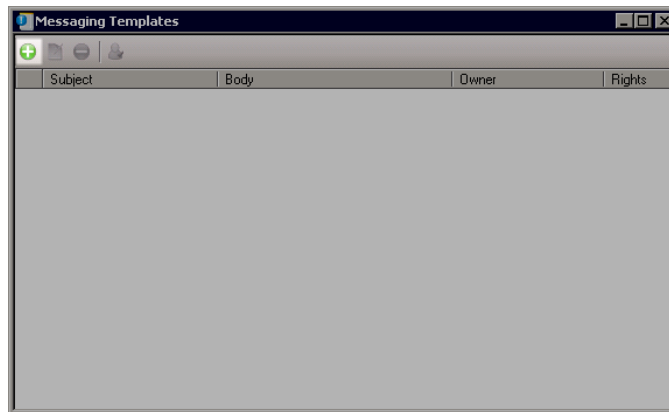
Creating Messaging Templates

When you create a Messaging Template, you can specify the list of users, the message subject, text, and priority, and an optional conversation expiration time. You can also supply a list of multiple choice responses for recipients to choose from.

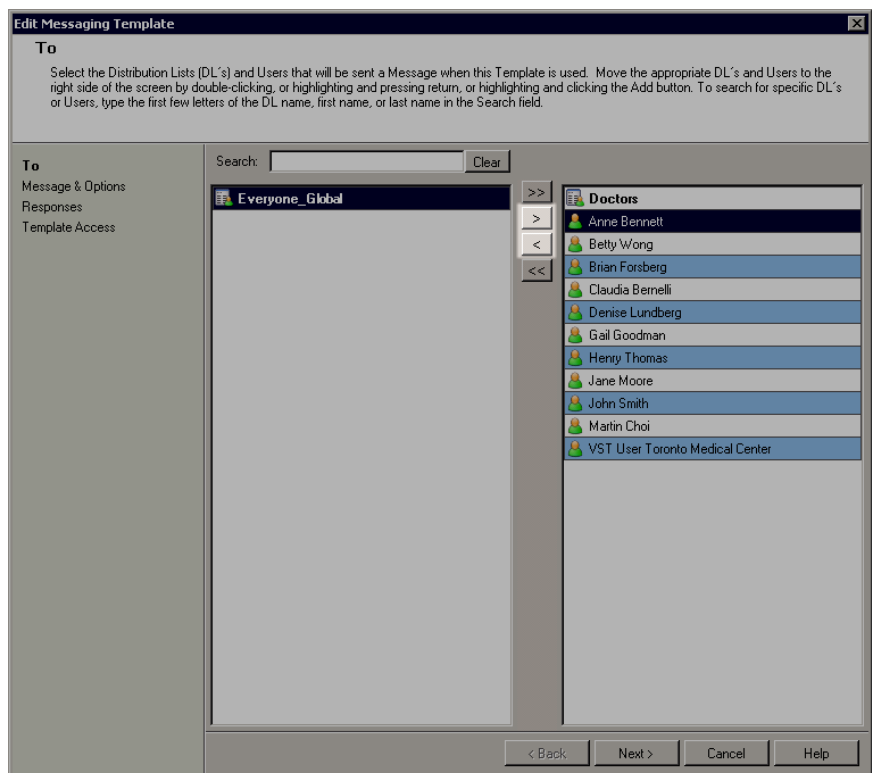
1. Open the VMP Administrator and select **Messaging > Messaging Templates**.



- Click New.



- Click to highlight each user or Distribution List that will receive a message when the template is used. Click > to add users and Distribution Lists to the list of recipients, or click < to remove them.



When you have finished adding users and Distribution Lists, click Next.



Note: The list of recipients can include only one Escalation Distribution List.

- Enter the following template details, and click Next:

Table 26: Messaging Template options

Option	Description
Subject	The subject line of the message. This can be up to 512 characters in length.
Message	The message text.

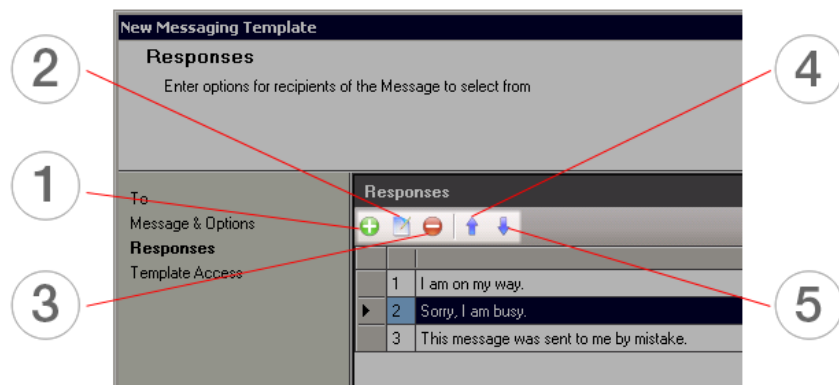
Option	Description
Priority	The message priority can be: <ul style="list-style-type: none"> • Urgent • High • Normal
Conversation expiration	The time in minutes before the message conversation expires. This can be one of the following: <ul style="list-style-type: none"> • Never (the default) • 2 min • 5 min • 10 min • Custom If you select <i>Custom</i> , a field appears in which you can specify the number of minutes.
Deliver to on campus users only	Select this checkbox if messages are to be sent only to recipients who are present.
Multiple Choice Responses	Select this checkbox if you want to define multiple choice responses for this template.

5. If you have selected *Multiple Choice Responses*, additional fields appear:

Table 27: Additional Messaging Template options

Option	Description
Notify if no one has responded	Select this checkbox if a notification is to be sent if no one has responded within the number of minutes that you specify.
Response expiration	The amount of time in which a response is expected. Select one of the following: <ul style="list-style-type: none"> • Never • 2 min • 5 min • 10 min • Custom - Enter the amount of time, in minutes, before the message expires.

6. If you selected *Multiple Choice Responses*, click *Next* to provide the response options.



1

Click *Add* to add a response. Type the text of the response in the dialog box provided, and click *OK*.

2

Click *Edit* to edit a response that you have created.

3

Click **Delete** to delete a response that you have created.

4

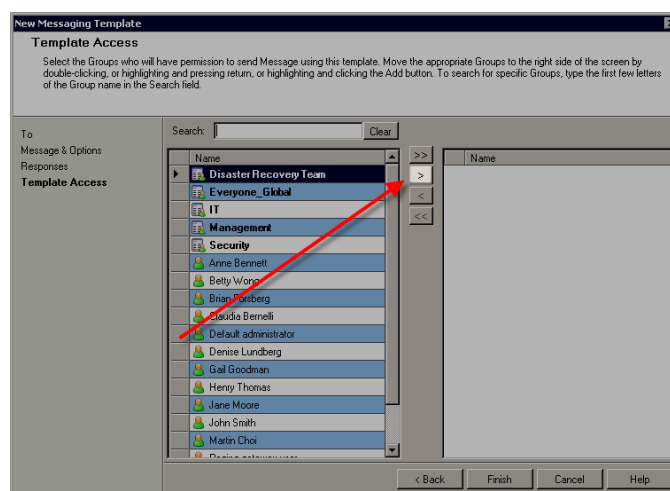
To rearrange the responses, click a response to highlight it. Click **Move Up** to move the response up in the list.

5

Click **Move Down** to move the response down. Repeat **Move Up** and **Move Down** until the responses are in the order that you want.

Click **Next** when you have finished creating message options.

- Click to highlight each user or group that can use the template, and click **>**.

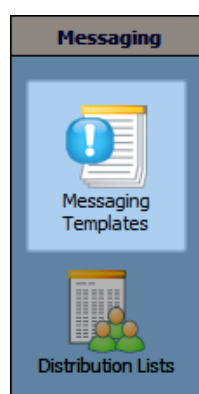


When you have finished adding groups, click **Finish**.

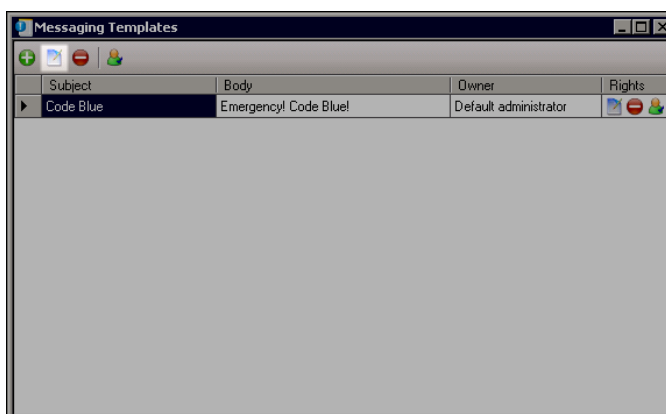
Editing a Messaging Template

You can edit any Messaging Template that you have created.

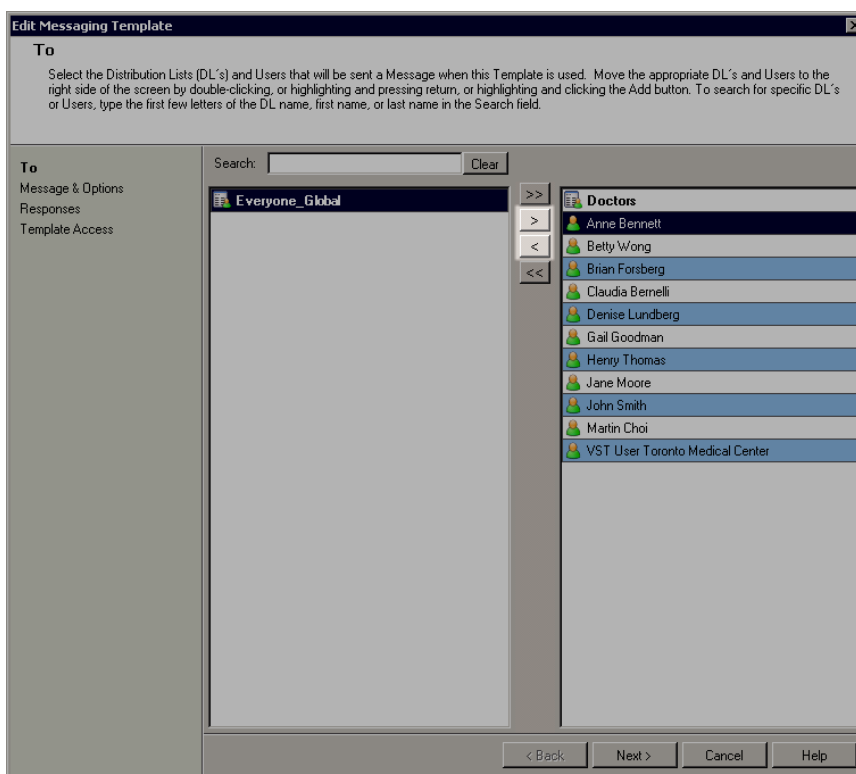
- In the VMP Administrator, select **Messaging > Messaging Templates**.



- Highlight the Messaging Template that you want to edit and click **Edit**.



- Click > to add users and Distribution Lists to the list of recipients, or click < to remove them.



When you have finished adding users and Distribution Lists, click Next.



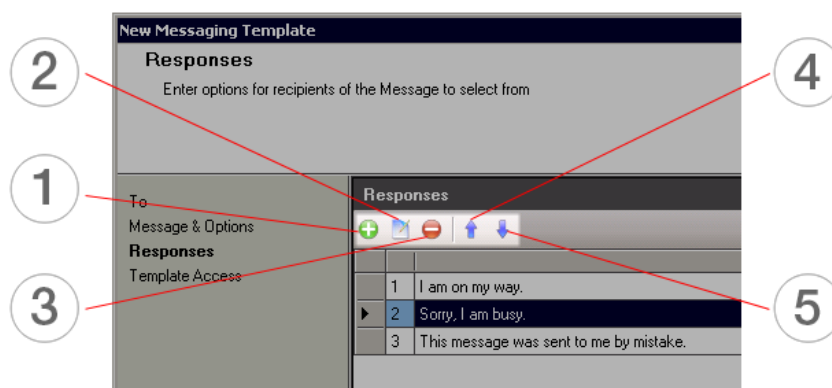
Note: The list of recipients can include only one Escalation Distribution List.

- Edit the messaging options as needed, and click Next when finished.



Note: For more information on these options, see [Creating Messaging Templates](#) on page 144.

- If you selected Multiple Choice Responses, you can update the response options.



1	Click Add to add a response. Type the text of the response in the dialog box provided, and click OK.
2	Click Edit to edit a response that you have created.
3	Click Delete to delete a response that you have created.
4	To rearrange the responses, click a response to highlight it. Click Move Up to move the response up in the list.
5	Click Move Down to move the response down. Repeat Move Up and Move Down until the responses are in the order that you want.

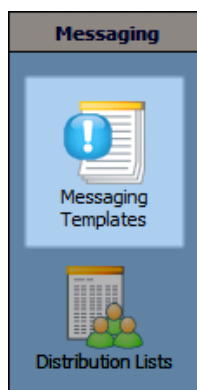
Click Next when you have finished updating message options.

6. To update the list of users or groups that can access the Messaging Template:
 - a. To add a user or group, highlight it in the left pane of the Template Access dialog and click >.
 - b. To remove a user or group, highlight it in the right pane and click <.
7. Click Finish when you have finished editing the Messaging Template.

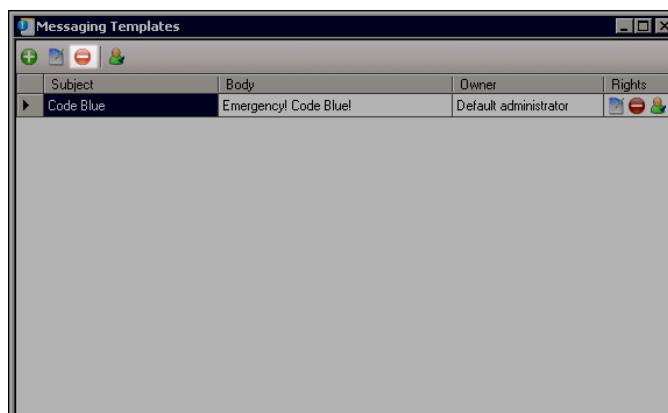
Deleting a Messaging Template

If you no longer need a Messaging Template, you can delete it.

1. In the VMP Administrator, select Messaging > Messaging Templates.



2. Highlight the Messaging Template that you want to delete and click Delete.

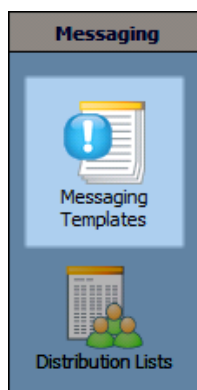


3. In the confirmation dialog box that appears, click Yes to confirm that you want to delete the Messaging Template.

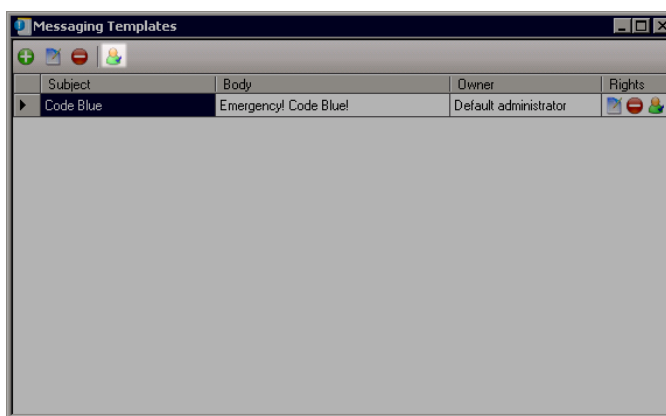
Changing Messaging Template Permissions

For any Messaging Template, you can specify the users that are allowed to update, delete, or manage access to the template.

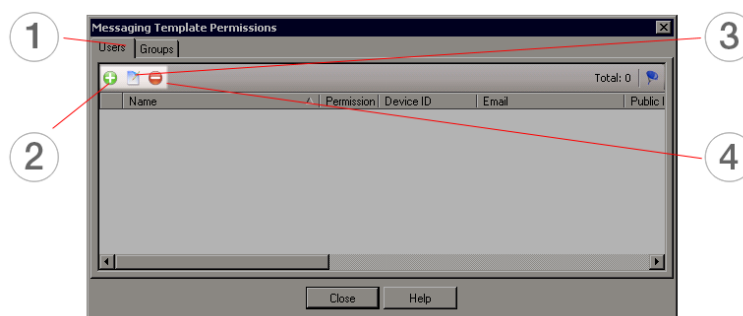
1. In the VMP Administrator, select Messaging > Messaging Templates.



2. Highlight the Messaging Template that you want to change permissions for, and click Manage access.



3. In the Messaging Template Permissions dialog box:



1

Click the Users tab to change permissions for users, or click the Groups tab to change permissions for groups.

2

Click Add to add a user or group to the list of users or groups with permissions. In the New Permission dialog box, highlight a user or group and click one or more permission checkboxes:

- **Allow update:** Members with this permission can add users to the list of message recipients, and can edit the message body, subject, and other Messaging Template properties.
- **Allow delete:** Members with this permission can remove this template.
- **Manage access:** Members with this permission can add or delete groups in the Messaging Template access list.

Click OK when done.

The default administrator has **Manage access** permission on every Messaging Template.

3

Click **Edit** to edit the permissions of a user or group.

4

Click **Delete** to delete from the list of users or groups with permissions.

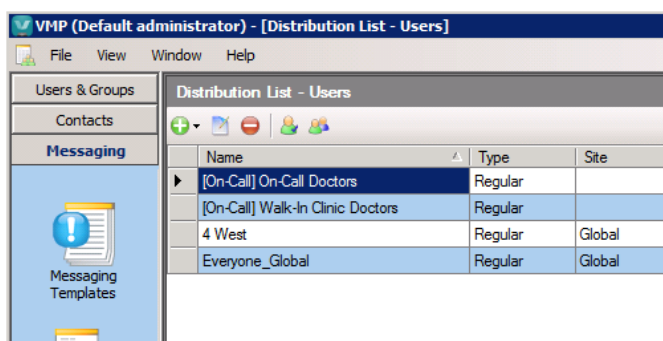
- Click **Close** to close the Messaging Template Permissions dialog box.

About Distribution Lists

In VMP, a Distribution List (DL) is a list of users. You can send a message to an entire DL, use a DL to set up an on-call roster, or create an Escalation Distribution List to ensure that your message is escalated if it is not seen by its initial recipients.

When you create a DL, you specify whether it is to be a Regular Distribution List or an Escalation Distribution List. An On-Call Distribution List, which you can use to create an on-call roster, is a special type of Regular Distribution List.

To display a list of all defined DLs, open the VMP Administrator application and select **Messaging > Distribution Lists**. The **Distribution List - Users** view appears.



In this view, On-Call Distribution Lists have the prefix **[On-Call]**, and Escalation Distribution Lists have the prefix **[Escalation]**. All other DLs are Regular Distribution Lists.

VMP automatically creates the following DLs:

- If your VMP Server is integrated with a Vocera Voice Server, the **Everyone_Global** DL is a copy of the **Everyone** group that is defined on your Vocera Voice Server. See [Vocera Voice Server Integration](#) on page 30 for more information on integrating with a Vocera Voice Server.
- If your VMP Server is integrated with Vocera Secure Texting, the **VST Users** DL lists all VST users. See [Vocera Secure Texting Integration](#) on page 35 for more information on integrating with VST.



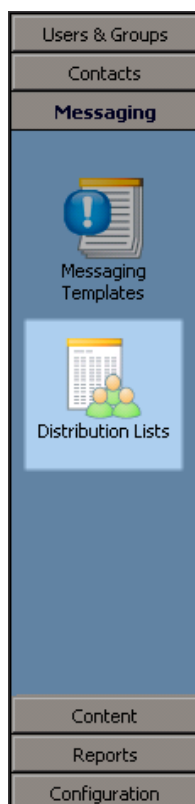
Note: VMP also enables you to define **Contacts Distribution Lists**, which are lists of contacts. See [Creating a Contacts Distribution List](#) on page 139 for more details.

Creating a Regular or On-Call Distribution List

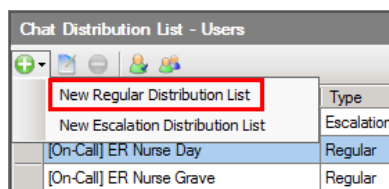
You can use the VMP Administrator to create a regular Distribution List (DL). You can specify that this regular DL is to be an On-Call Distribution List.

A regular DL is any DL other than an Escalation Distribution List, which is a special case that is created separately.

- Open the VMP Administrator application and select **Messaging > Distribution Lists**.



- Click New and select New Regular Distribution List.



- In the Distribution List Name field, enter the name of the new DL.
- In the Distribution List ID field, enter the ID of the new DL.



Note: When a message is initiated by an external system such as email or WCTP, VMP uses this ID to determine the DL to which the message is to be sent.

- If this Distribution List is to be associated with a site, select the site from the Site dropdown list.



Note: Sites are available if they have been created on the Vocera Voice Server with which the VMP Server has been integrated. See [Vocera Voice Server Integration](#) on page 30 for more information on integrating with the Vocera Voice Server.

- Select Enable for Texting if you want this DL to be available to Messaging users.
- If Enable for Texting is selected, you can select On-Call Distribution List to ensure that DL members receive messages only if their status is On-Call or Monitor. In the Minimum Users On-Call field, select or type the minimum number of users that can be On-Call at any one time.



Note: If a user is having messages forwarded, the user can still be On-Call.

- Select Hidden if this DL is to remain hidden. Users can send messages to members of a hidden DL, but cannot send a message to the DL itself.
- Select how users can be added to the DL. You can select either Add Users Manually or Create DL based on Active Directory structure.

10. Click Next.

11. If you have selected **Add Users Manually**:

- Type in the **Search** field to display only users whose names contain the search string. Click **Clear** to clear the search string.
- Select **All Users** to display all users, or select **VST Users** to display Vocera Secure Texting users only. You can do this for either the list of users that have not yet been added to the DL or the list of users that have been added.



Note: For more information on importing Vocera Secure Texting users into VMP, see [Enabling VST Message Exchange](#) on page 35.

- Click to highlight a user, and then click **>** to move the user to the Distribution List. You can click to highlight one or many users. To move all users to the Distribution List, click **>>**.

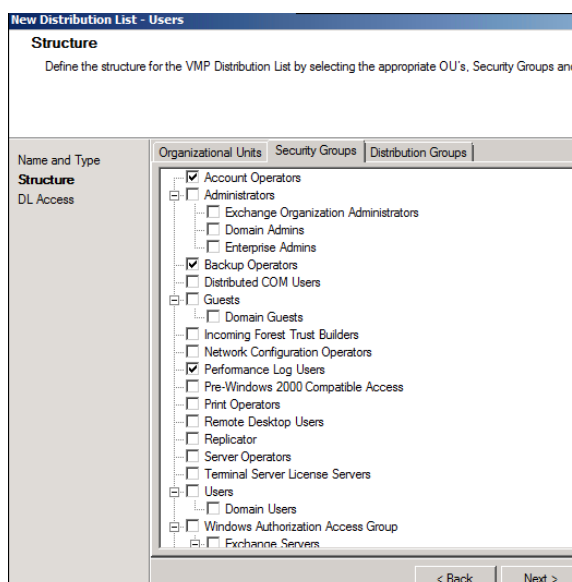
d. If the DL is an On-Call DL:

- Select **Edit Personal On-Call Status** to let users edit their own on-call status.
- Select **Edit On-Call Status For All** to let users manage the on-call status for all members of the DL.
- In the **Current On-Call Status** dropdown list, specify the on-call status for each user. Select **Not On-Call**, **Monitor**, or **On-Call**.

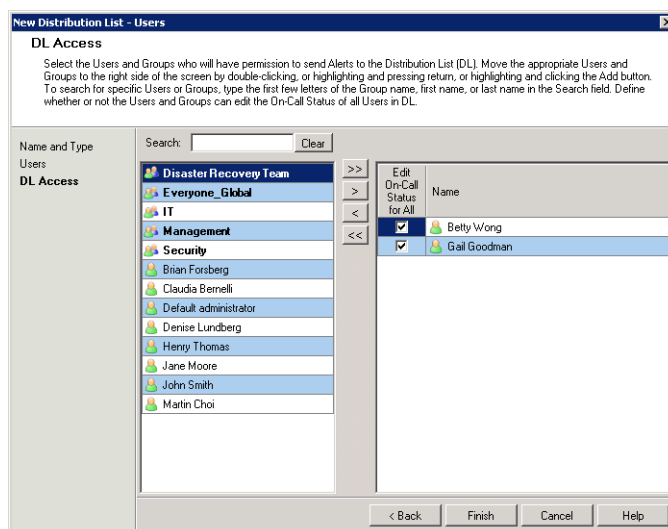
Edit Personal On-Call Status	Edit On-Call Status for All	Current On-Call Status	Name
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Not On-Call	Betty Wong
<input checked="" type="checkbox"/>	<input type="checkbox"/>	On-Call	Brian Forsberg
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Monitor	Claudia Bernelli
		Not On-Call	

e. Click Next.

12. If you are creating the DL from an existing Active Directory structure, select the users and groups from the tabbed lists, and click Next.



13. The DL Access window appears, which lets you select the users and groups who will have permission to send messages to this DL.



Type in the Search field to display only users whose names contain the search string. Click Clear to clear the search string.

14. Click to highlight a user, and then click > to give the user permission to send a message to this Distribution List. You can click to highlight one or many users. To give all users permission to send messages, click >>.
15. If the new list is an On-Call Distribution List, select the Edit On-Call Status for All checkbox next to each user who is to be given permission to edit anyone's on-call status.



Note: If a user is both a member of a DL and has permission to send a message to the DL, you can select the Edit On-Call Status for All checkbox in either this screen or the Users screen. Selecting either checkbox enables the ability to edit anyone's on-call status.

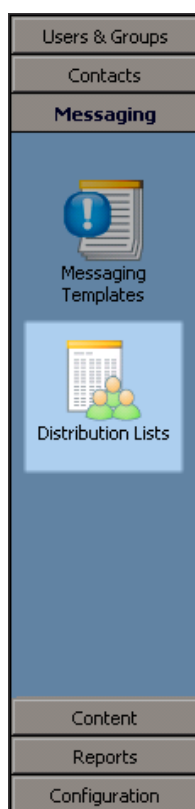
16. Click Finish to create the DL.

Creating an Escalation Distribution List

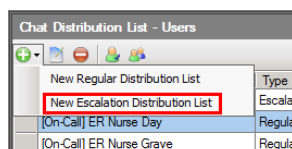
Use Escalation Distribution Lists to improve message response times by forwarding the message through a defined escalation workflow.

For each list, one or more branches of groups or users are defined. When a message is sent to the list, it is sent to the first branch. If no one in the first branch responds in the specified time, the message is escalated to the next branch. It is then escalated to additional branches if necessary.

1. Open the VMP Administrator application and select **Messaging > Distribution Lists**.



2. Click **New** and select **New Escalation Distribution List**.



3. In the **Distribution List Name** field, enter the name of the new DL.
4. In the **Distribution List ID** field, enter the ID of the new DL.



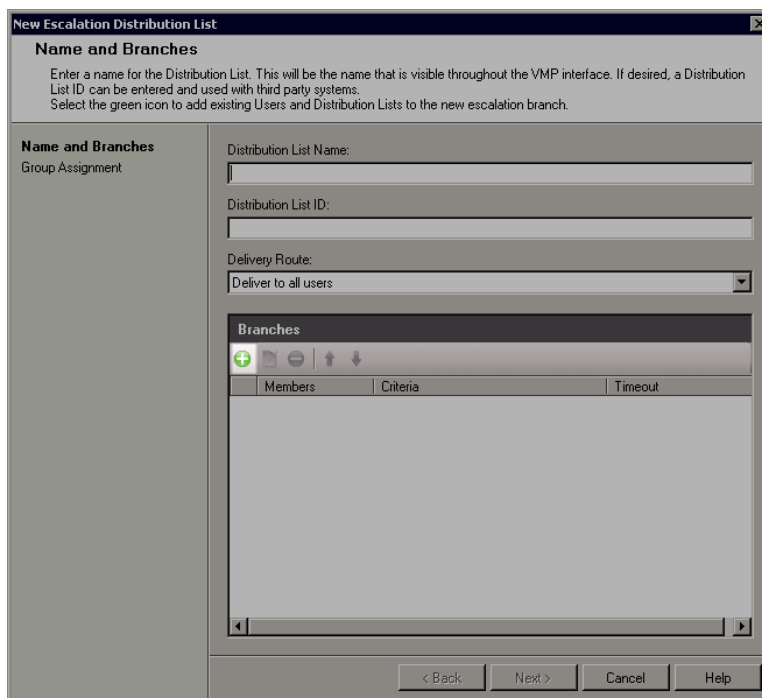
Note: When a message is initiated by an external system such as email or WCTP, VMP uses this ID to determine the DL to which the message is to be sent.

5. Use the **Delivery Route** dropdown list to select from one of the following options:

Table 28: Delivery route options

Option	Description
Deliver to all users	Deliver to all DL members.
Deliver only to users who are present on the Wi-Fi network.	Messages sent to the DL are delivered only to active members who are currently logged onto the Vocera Voice Server and are not in DND mode.
	 Note: If a user is present on the Wi-Fi network, but is forwarding messages to a user who is not present, the message is not delivered.

6. Next, create the branches for the Escalation Distribution List:
 - a. Click **New** to add a **New Branch** to the Escalation Distribution List.



New Escalation Distribution List

Name and Branches

Enter a name for the Distribution List. This will be the name that is visible throughout the VMP interface. If desired, a Distribution List ID can be entered and used with third party systems.
Select the green icon to add existing Users and Distribution Lists to the new escalation branch.

Name and Branches
Group Assignment

Distribution List Name:

Distribution List ID:

Delivery Route:

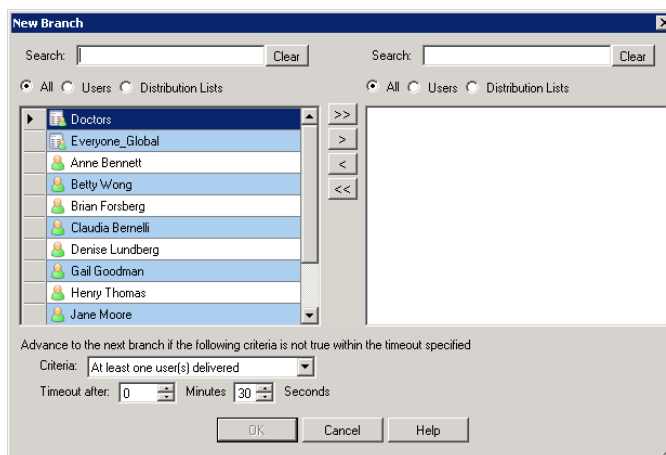
Branches

Members	Criteria	Timeout

< Back Next > Cancel Help

Each branch contains one set of users to be contacted. If the response criteria are not met, the Escalation Distribution List escalates to the next branch.

- b. In the New Branch dialog box, type in the Search field to display only users whose names contain the search string. Click Clear to clear the search string.



New Branch

Search: Clear Search: Clear

☒ All ☐ Users ☐ Distribution Lists ☒ All ☐ Users ☐ Distribution Lists

Doctors	
Everyone_Global	
Anne Bennett	
Betty Wong	
Brian Forsberg	
Claudia Bernelli	
Denise Lundberg	
Gail Goodman	
Henry Thomas	
Jane Moore	

Advance to the next branch if the following criteria is not true within the timeout specified

Criteria:

Timeout after: Minutes Seconds


OK Cancel Help

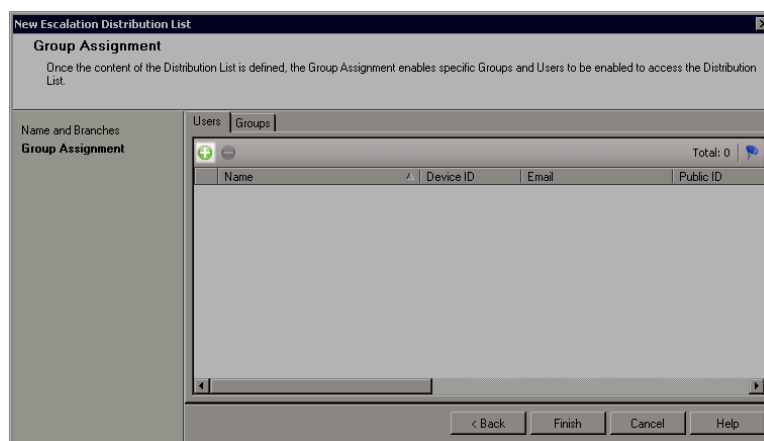
- c. Filter the selection criteria using one of the following options:
- All
 - Users
 - Distribution Lists



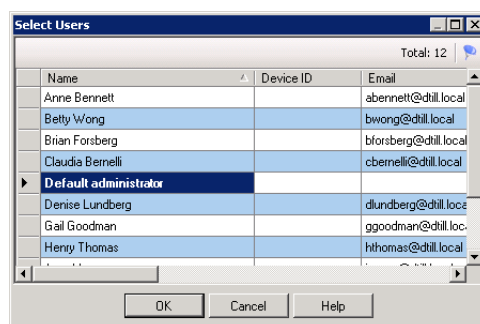
Note: If a search string has been specified, only users whose names contain the search string are listed.

- d. Click to highlight a user, and then click > to move the user to the new branch of the Escalation Distribution List. You can click to highlight one or many users. To move all users to the new branch, click >>.
- e. Use the Criteria dropdown list to specify the response criteria. If these criteria are not met, the message is escalated. The available response criteria are:
- At least one user(s) delivered
 - At least one user(s) opened

- At least one user(s) responded
 - All users delivered
 - All users opened
 - All users responded
- f. Set the timeout value and click **OK** to continue. The timeout value must be 5 seconds or greater.
-  **Note:** When a message is sent to an Escalation Distribution List, and all members of a branch of the list are off campus, the message is immediately escalated to the next branch of the list without waiting for the timeout period to elapse.
- g. Repeat these steps as necessary to create additional branches.
7. Click **Next**. The Group Assignment window appears, which lets specific users and groups access the DL.
8. Click the **Users** tab to add a user to the access list, or click **Groups** to add a group:
- a. Click **Add** to display a list of users or groups.



The Select Users or Select Groups window appears.

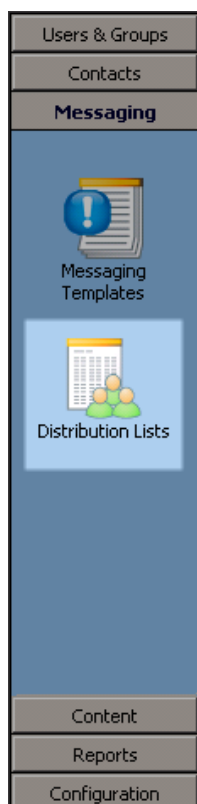


- b. Select one or more users or groups from the list.
- c. Click **OK** to add the users or groups to the list.
- d. Repeat the above steps to add additional users or groups.
9. Click **Finish** to create the DL.

Editing a Distribution List

You can edit any Distribution List or Escalation Distribution List that you have created.

1. Open the VMP Administrator application and select **Messaging > Distribution Lists**.

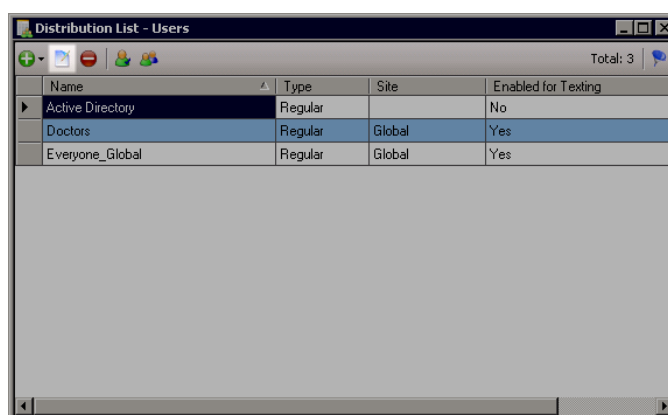


2. Click the name of a Distribution List to select it.



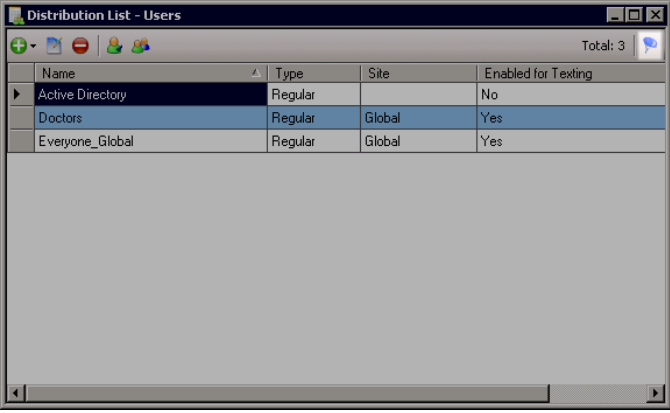
Note: On-Call Distribution Lists are labeled with the prefix [On-Call]. Escalation Distribution Lists are labeled with the prefix [Escalation].

3. Click Edit.



4. The instructions for editing a Distribution List are the same as those for creating a list:
 - If you are editing a regular Distribution List, see [Creating a Regular or On-Call Distribution List](#) on page 152.
 - If you are editing an Escalation Distribution List, see [Creating an Escalation Distribution List](#) on page 155.

To filter the list of Distribution Lists, click [Filter](#) and enter the filtering criterion to use.



The screenshot shows a window titled "Distribution List - Users" with a toolbar at the top containing icons for adding, deleting, and refreshing. A status bar at the top right indicates "Total: 3". Below the toolbar is a table with the following data:

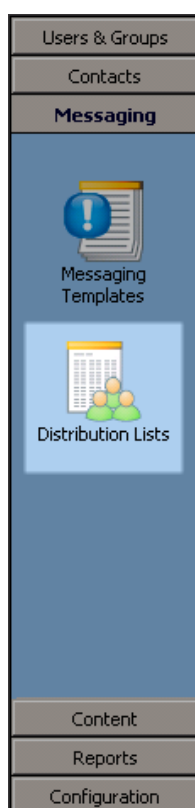
Name	Type	Site	Enabled for Texting
Active Directory	Regular		No
Doctors	Regular	Global	Yes
Everyone_Global	Regular	Global	Yes

The Filter icon changes color. To reset filtering, right-click Filter.

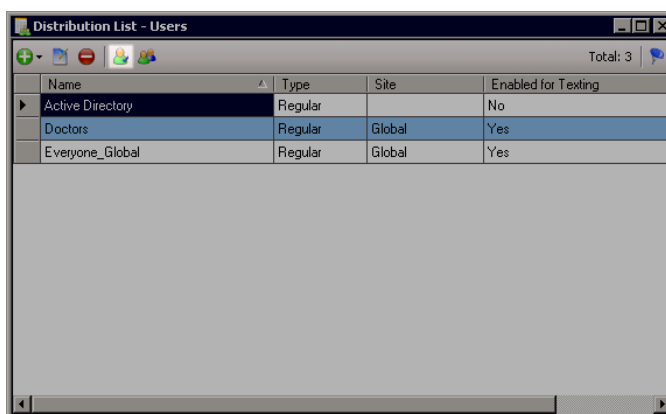
Managing Access to a Distribution List

After you have created a Distribution List, you can specify users that can access the list.

1. Open the VMP Administrator application and select **Messaging > Distribution Lists**.

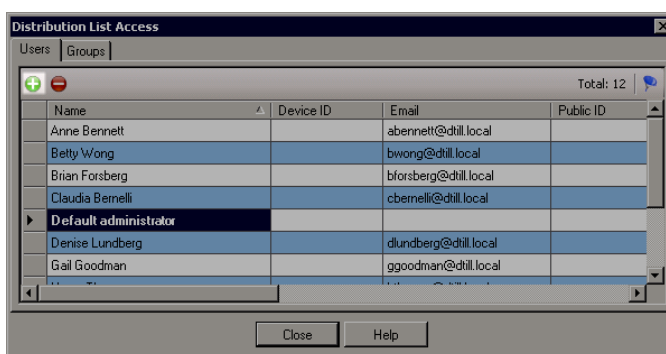


2. Click the name of a Distribution List or Escalation Distribution List to select it.
3. Click **Manage Access**.



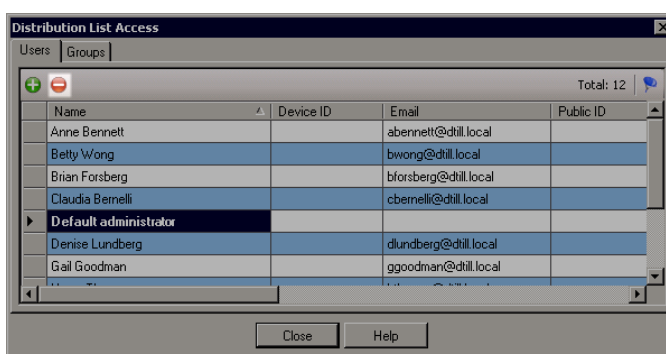
The Distribution List Access dialog box appears.

- To add users or groups that can access the list, click Add.



In the dialog box that appears, click the Users or Groups tab, click the names of the users or groups to add, and then click OK.

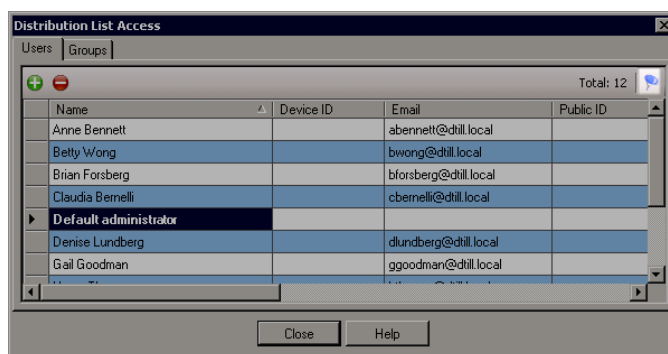
- To remove access to the list, click the Users or Groups tab, click the names of the users or groups whose access is to be removed, and then click Delete.



When asked whether you want to remove these users or groups, click Yes.

- When you have finished updating user access, click Close.

To filter the list of users in the Distribution List Access dialog box, click Filter and enter the filtering criteria to use.

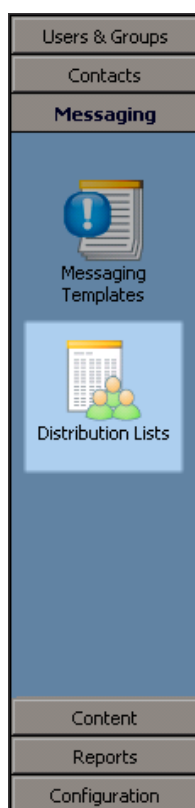


The Filter icon changes color. To reset filtering, right-click Filter.

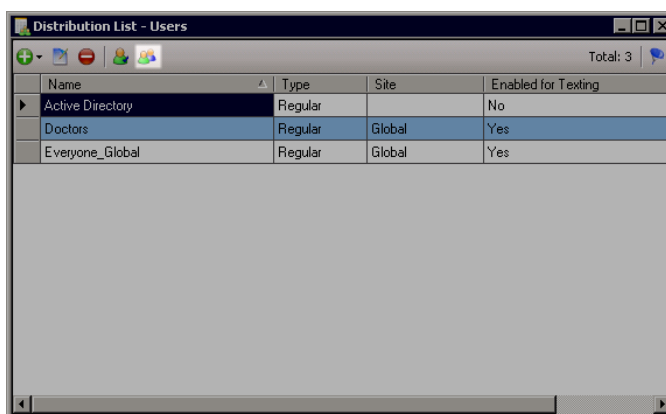
Viewing the Members of a Distribution List

You can view a list of all members of any existing Distribution List.

1. Open the VMP Administrator application and select **Messaging > Distribution Lists**.



2. Click the name of a Distribution List or Escalation Distribution List to select it.
3. Click **View Members**.



A dialog box appears, containing a list of Distribution List members.

Additional fields are displayed with this list of members, depending on the type of DL:

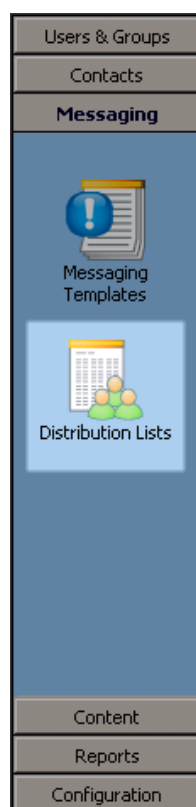
- For Regular DLs created in VMP, this dialog box lists the Device ID, email address, and Public ID for each user.
- For DLs imported from Vocera groups, the status for each user is displayed.
- For Escalation DLs, the branch number is displayed.

4. Click **OK** to close the dialog box.

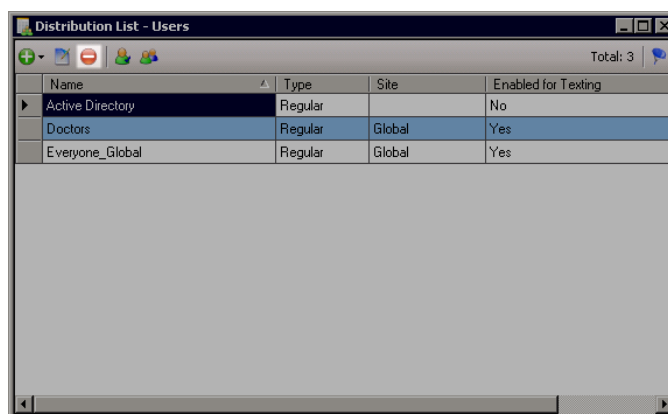
Deleting a Distribution List

If you no longer need a Distribution List, you can delete it.

1. Open the VMP Administrator application and select **Messaging > Distribution Lists**.



2. Click the name of a Distribution List or Escalation Distribution List to select it.
3. Click **Delete**.



- In the dialog box that appears, click **Yes** to confirm that you want to delete the list.

Content

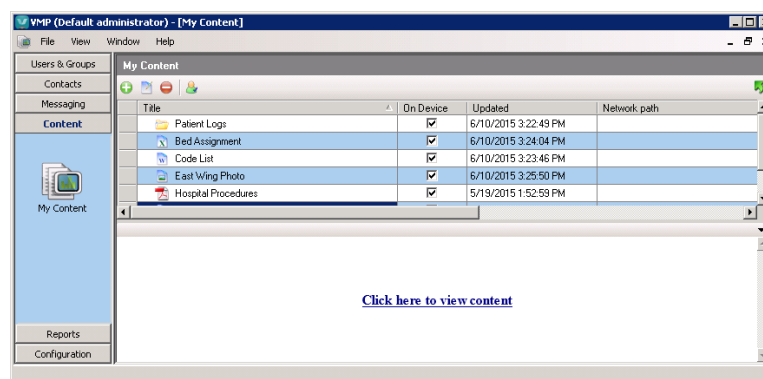
The Content module provides the tools to manage documents and image files that are stored on the VMP Server and can be distributed and shared with licensed devices. It can deliver floor-plans, forms, and other essential team documents.

Content is uploaded and managed by the administrator. When a file is uploaded to the VMP Server, the title and upload date are posted to the main screen of the console. VMP supports the following file types:

- HTML file
- Image file (JPEG, GIF, BMP and PNG)
- PDF file
- Microsoft Word document
- Excel document
- Text
- Audio and video

If you plan to distribute Microsoft Word and Excel documents, you must have Microsoft Word and Excel installed on your server so that it can properly format the documents for the device. For audio and video, all content is streamed, and client devices can play all files that are supported by their media players.

The My Content view provides a list of the current documentation in the configured hierarchy.



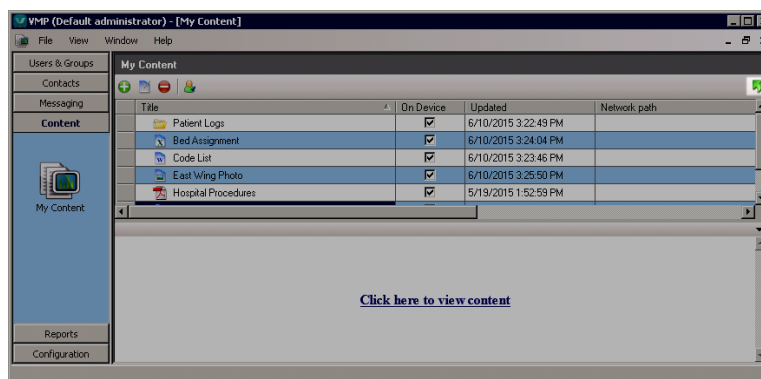
Features of this view include:

- Content view window
- Activate or deactivate device presence
- Content update timestamp

- Network path information



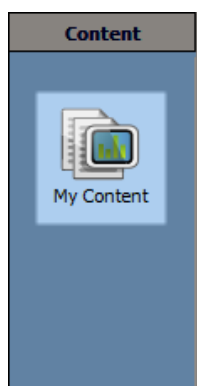
Note: To refresh the list of available content displayed in the Content module, click Refresh.



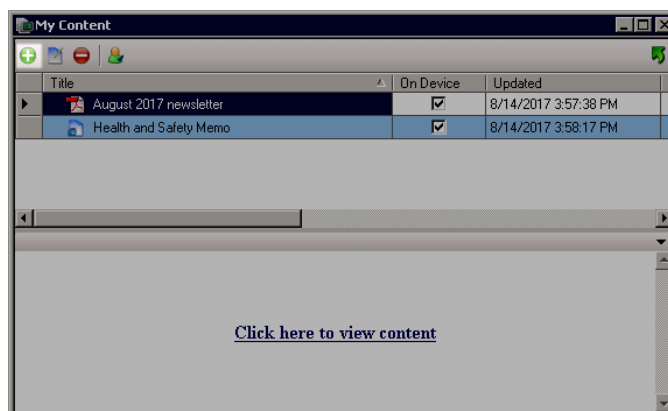
Adding Content

You can use the VMP Administrator to add new content that can be made available to client devices.

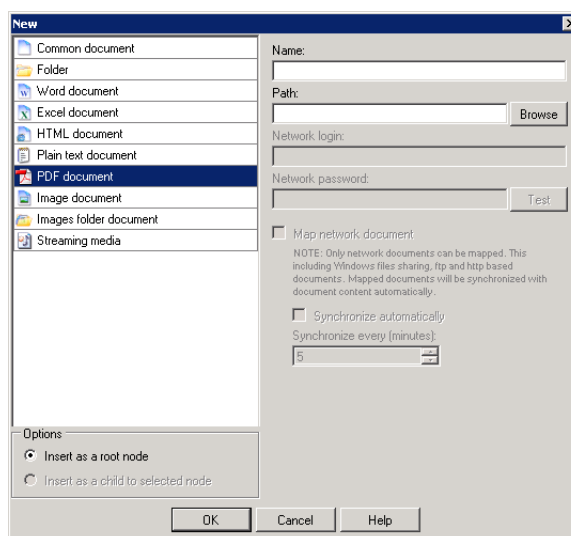
1. Open the VMP Administrator application and select Content > My Content.



2. If you are adding content to an existing folder, or as a child of an existing content instance, click to highlight the folder or instance.
3. Click Open to open the New Content view.



4. Click to highlight the document type and click Browse to select the new document.



Note: The Name field contains the document name, and it auto-populates based on the selected document. If you enter a name in the Name field, it will persist.

5. If the document resides on a network that requires credentials, use the Network login and Network password fields to enter the credentials.
6. Optionally, you can select Map network document. Mapping allows you to configure automatic synchronization for document updates. If desired, select this option and configure a synchronization interval.



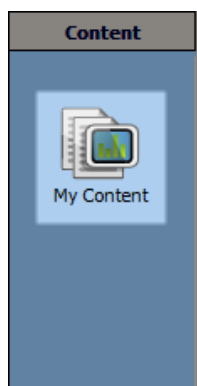
Note: If your documents reside on a remote network, automatic synchronization will not work unless the Vocera Data Exchange service is modified to use a local administrator account instead of the default VMP Local System account.

7. If the document type you have selected is Word document or HTML document, the Document style dropdown list appears. Select the document style to use.
8. If the document type you have selected is Word document, Excel document, or HTML document, the Use first tables row as column names dropdown list appears. Select one of the following:
 - Yes - Use the entries in the first row of the table as the column names.
 - No - Do not use table row entries as column names.
 - Use parent folder settings - Use the settings specified in the parent folder.
9. In the Options section, select Insert as a root node to insert the new document into the My Content folder, or select Insert as a child to selected node to insert the new document into the selected folder.
10. Click OK to close the dialog and upload the document to the server.

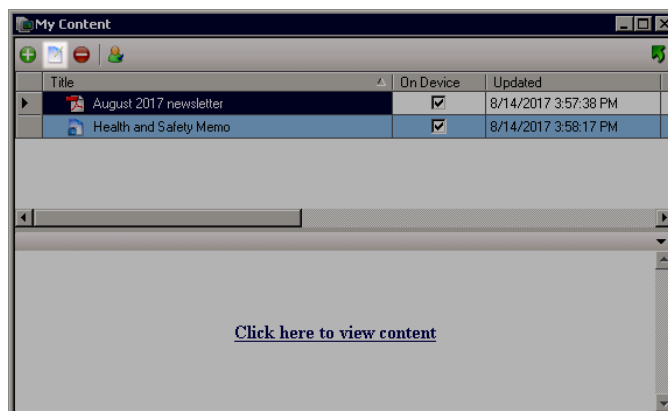
Updating Content

If necessary, you can update content that you have already uploaded to the VMP Server.

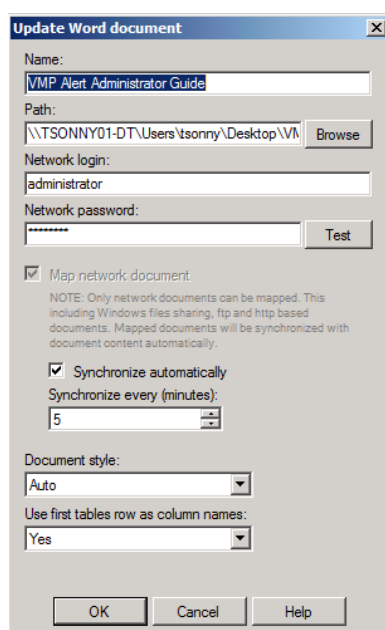
1. Open the VMP Administrator application and select Content > My Content.



2. Click to highlight the folder or document, and select Edit.



3. If the document is a Word document or an HTML document, from the Document style dropdown list, select the document style to use.
4. If the document is a Word document, an Excel document, or an HTML document, from the Use first tables row as column names dropdown list, select one of the following:
 - Yes – Use the entries in the first row of the table as the column names.
 - No – Do not use table row entries as column names.
 - Use parent folder settings – Use the settings specified in the parent folder.
5. Click OK to save your changes.

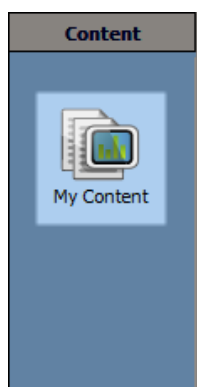


Assigning Document Permissions

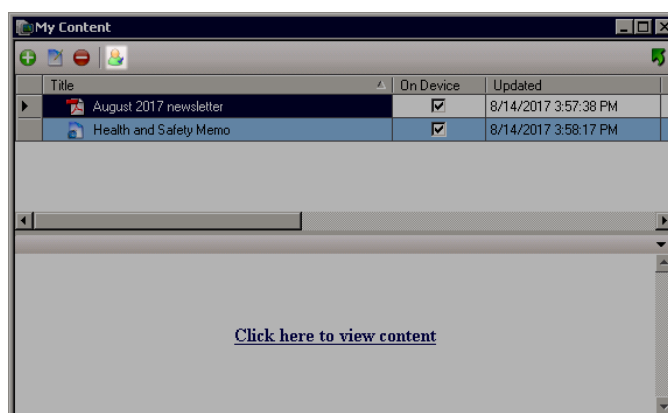
You can use document permissions to specify the content that is to be made available to any client device user.

Use the following steps to define document privileges.

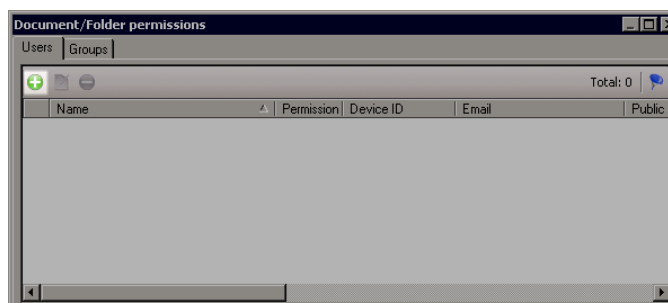
1. Open the VMP Administrator application and select **Content > My Content**.



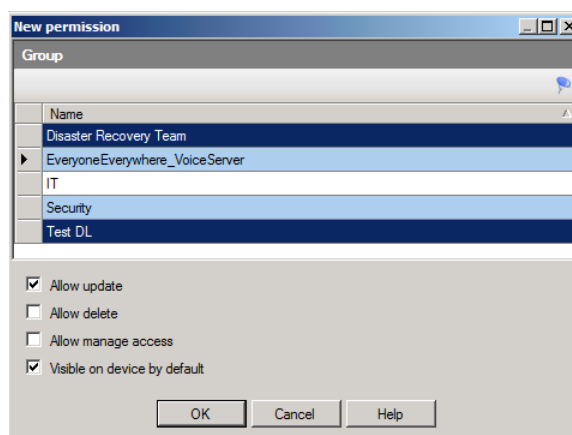
2. Click to highlight the folder or document, and select **Manage Permissions**.



3. Choose the **Users** or **Groups** tab, and select **New**.

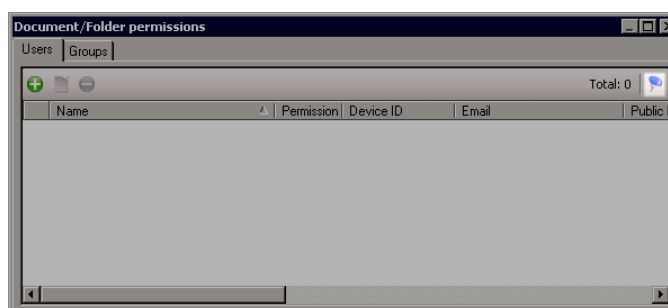


4. Click to highlight one or more entries.
5. Select one or more of the following permission options:
 - Allow updates
 - Allow delete
 - Allow manage access
 - Visible in device by default



6. Click OK.

To filter the list of entries, click Filter.

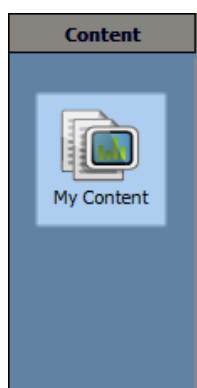


To reset filtering, right-click Filter.

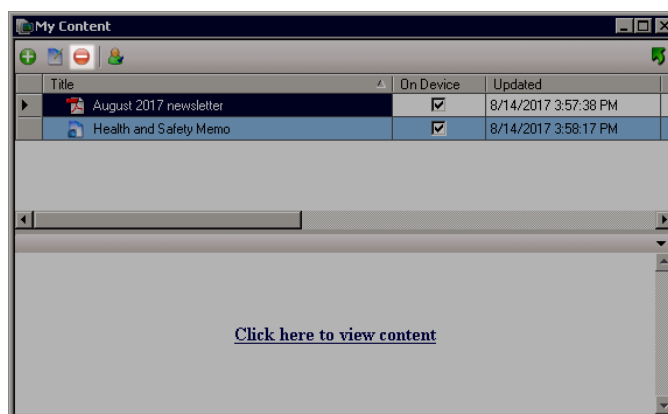
Deleting Content

You can delete content that you have added.

1. Open the VMP Administrator application and select Content > My Content.



2. Click to highlight the folder or document, and select Delete.
3. In the Delete Documents / Folders dialog, click Yes to confirm that you want to delete the content.



Reports

The Reports module gives Vocera administrators the ability to customize reports for organizational requirements such as audits and quality of service. Administrators can generate a report at any time and filter specific messaging details.

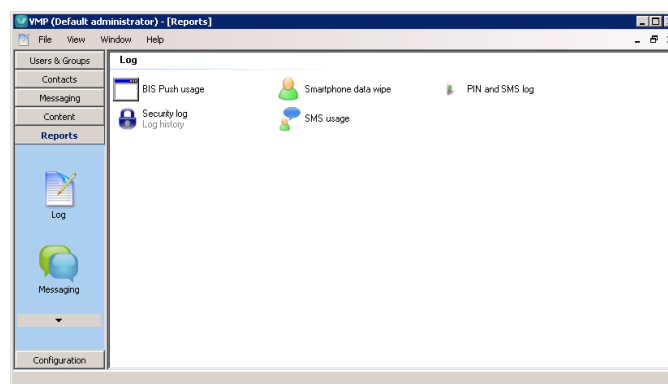
The following categories of reports are available:

- Log
- Messaging
- Transmit Status

About Logging Reports

In the Reports module, you can display the logging reports that can be generated.

To display the logging reports, select the **Log** icon.



The following Log reports can be generated:

Table 29: Log reports

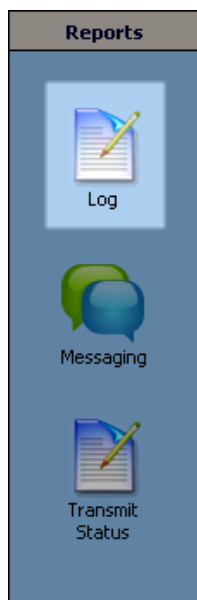
Report Type	Description
BIS Push usage	This legacy report provides the number of BlackBerry Push API messages sent by the server.
Smartphone data wipe	This lets Administrators view whether a data wipe was successful when sent to a device. This report is the only way to determine the status of a sent device deletion.
PIN and SMS log	This legacy report displays the BlackBerry PIN and SMS log by selected time frame.
Security log	Provides a record of Administrator actions. The report can record actions such as include logging in and out, creating users, and the deletion of contacts, Distribution Lists, groups, or other server entities.

Report Type	Description
SMS usage	Shows the SMS usage of a device.

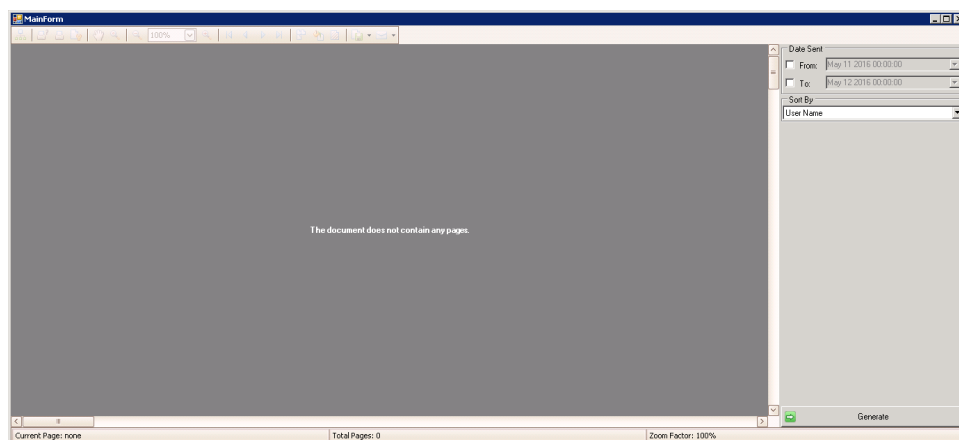
Creating a Smartphone Data Wipe Report

You can generate a report that indicates whether a data wipe was successful when sent to a device.

1. Open the VMP Administrator application and select **Reports > Log**.



2. In the Reports pane, click **Smartphone data wipe**. The **Smartphone Data Wipe Report** window opens.

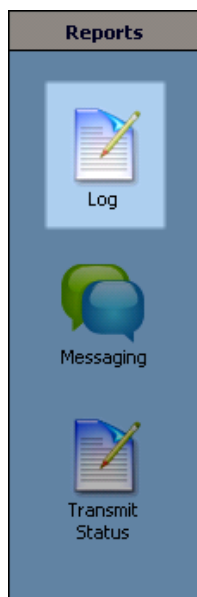


3. In the **Date** section, in the **From** field, select the start date for which wipe data is to be displayed. The default is midnight at the start of today's date.
4. In the **To** field, select the end date for wipe data. The default is midnight at the start of the next day's date.
5. From the **Sort By** dropdown list, select one of the following:
 - **User Name**: sort by user name,
 - **Kill Pill Generated timestamp**: sort by the date on which the smartphone wipe request was sent.
 - **Kill Pill Acknowledged timestamp**: sort by the date on which the smartphone wipe request was acknowledged.
6. Click **Generate** to generate the security log report.

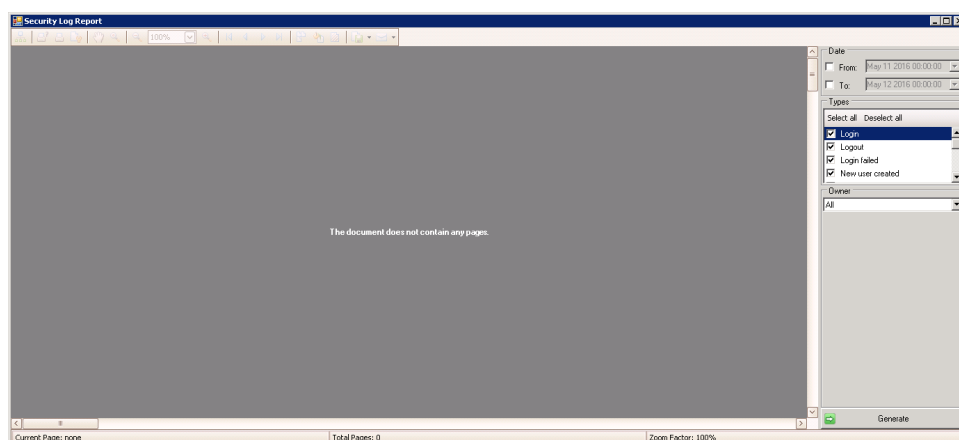
Creating a Security Log Report

You can generate a report that produces a security log. This log lists when users were created, all attempts to log in and log out, and all changes made in the VMP Server.

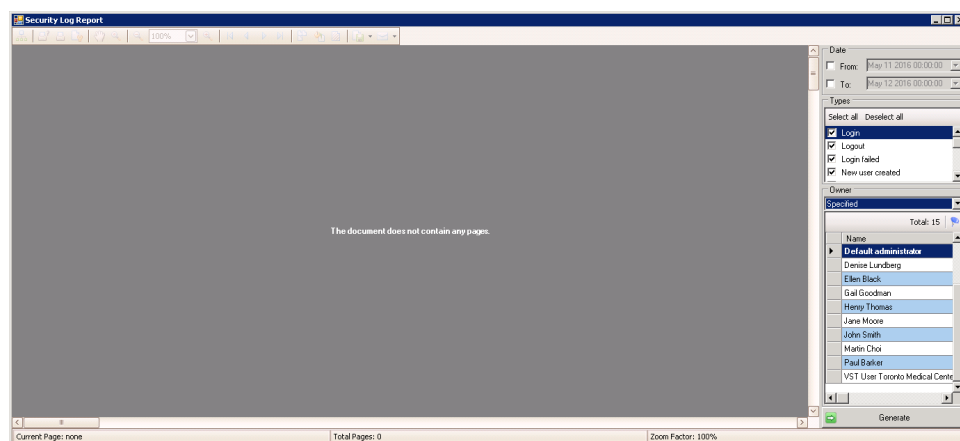
1. Open the VMP Administrator application and select **Reports > Log**.



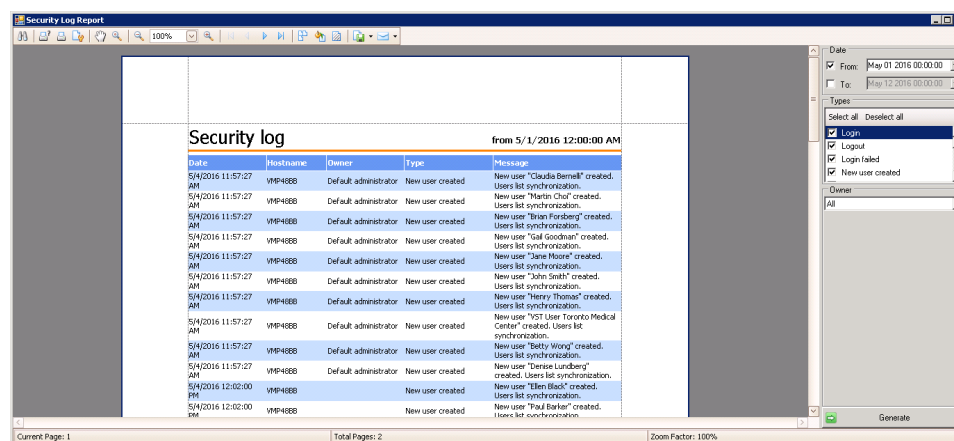
2. In the Reports pane, click **Security log**. The Security Log Report window opens.



3. In the **Date** section, in the **From** field, select the start date for which log information is to be displayed. The default is midnight at the start of today's date.
4. In the **To** field, select the end date for log information. The default is midnight at the start of the next day's date.
5. In the **Types** section, select the checkboxes next to the log activities that are to be included in the report. Click **Select all** to select all checkboxes, or click **Deselect all** to clear all checkboxes.
6. From the **Owner** dropdown list, select one of the following:
 - **All**: display security log information for all users,
 - **Selected**: specify the users for which you want to display information.
 - **Unknown user**: display security log information for unknown users only.
 - a. If you select **Selected**, a list of users appears. Select the users for which you want to display security log information.



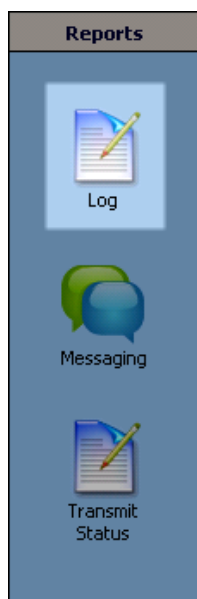
7. Click Generate to generate the security log report.



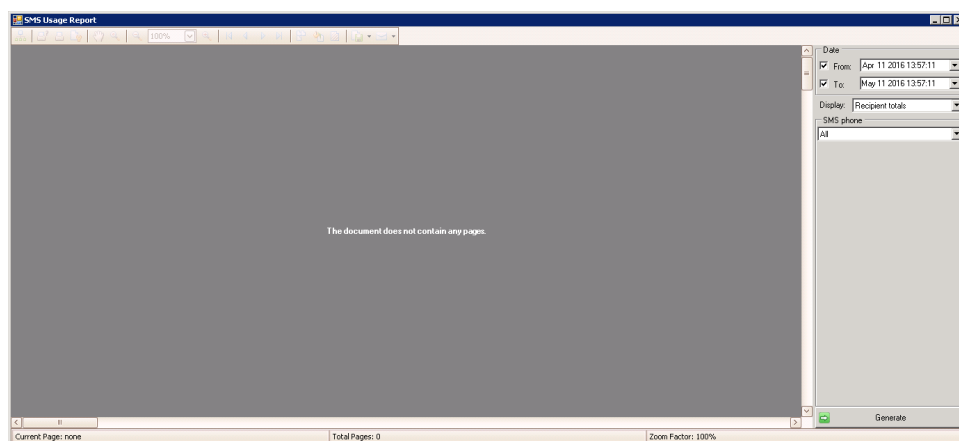
Creating an SMS Usage Report

You can generate a report that shows the SMS usage for each device.

1. Open the VMP Administrator application and select Reports > Log.



2. In the Reports pane, click SMS usage. The SMS Usage Report window opens.

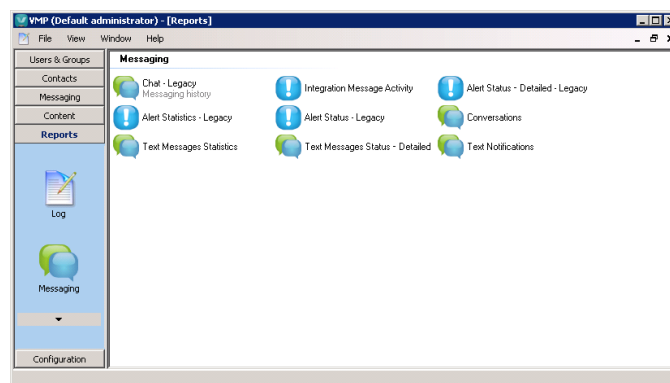


3. In the **Date** section, in the **From** field, select the start date for which log information is to be displayed. The default is midnight at the start of today's date.
4. In the **To** field, select the end date for log information. The default is midnight at the start of the next day's date.
5. From the **Display** dropdown list, select either **Recipient totals** or **Total only**.
6. From the **SMS phone** dropdown list, select either **All** or **Specified**. If you select **Specified**, select the SMS phones whose information you want to display.
7. Click **Generate** to generate the SMS usage report.

About Messaging Reports

In the Reports module, you can display reports that list the messaging history, statuses, and statistics for the VMP Server.

To display these reports, select the **Messaging** icon.



The following Messaging reports can be generated:

Table 30: Messaging reports

Report Type	Description
Chat - Legacy	For clients that have used the legacy Chat capability that was provided in previous versions of VMP, this displays a timestamp of each Chat message and provides the sender name, participants, images, and message details.
Integration Message Activity	This report is not currently in use.
Alert Status - Detailed - Legacy	For clients that have used the legacy Alert capability that was provided in previous versions of VMP, this displays specific details for Alerts sent to any device.

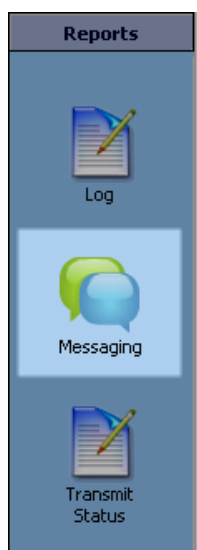
Report Type	Description
Alert Statistics - Legacy	For clients that have used the legacy Alert capability that was provided in previous versions of VMP, this displays information on all Alerts sent in a specified time period.
Alert Status - Legacy	For clients that have used the legacy Alert capability that was provided in previous versions of VMP, this displays the Alert statuses for any user. Select the user from the user filter that appears when the report screen is displayed.
Conversations	Displays the conversations or text messages for any user.
Text Messages Statistics	Displays information on all text messages sent in a specific time period.
Text Messages Status - Detailed	Displays specific details for text messages sent to any device.
Text Notifications	Displays the text notifications for any user. Select the user from the user filter that appears when the report screen is displayed.

The reports that are not legacy reports from previous versions of VMP are described in more detail below.

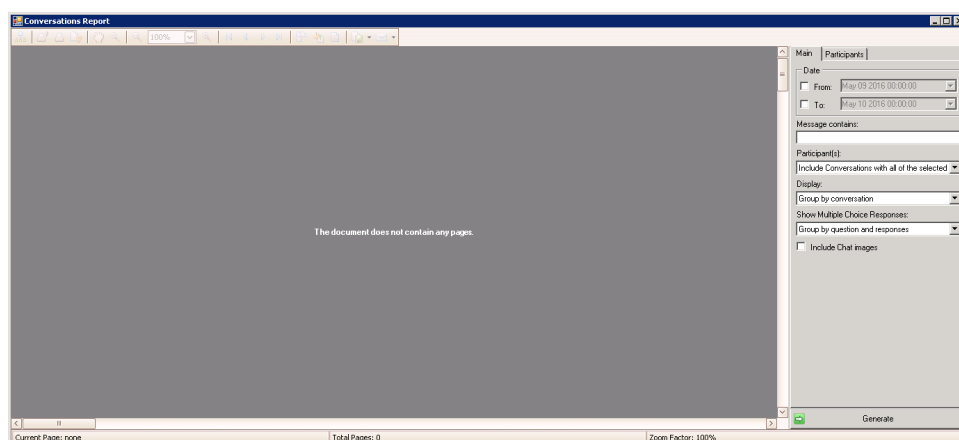
Creating a Conversations Report

You can generate a report that displays the conversations or text messages for any user or group of users.

1. Open the VMP Administrator application and select **Reports > Messaging**.

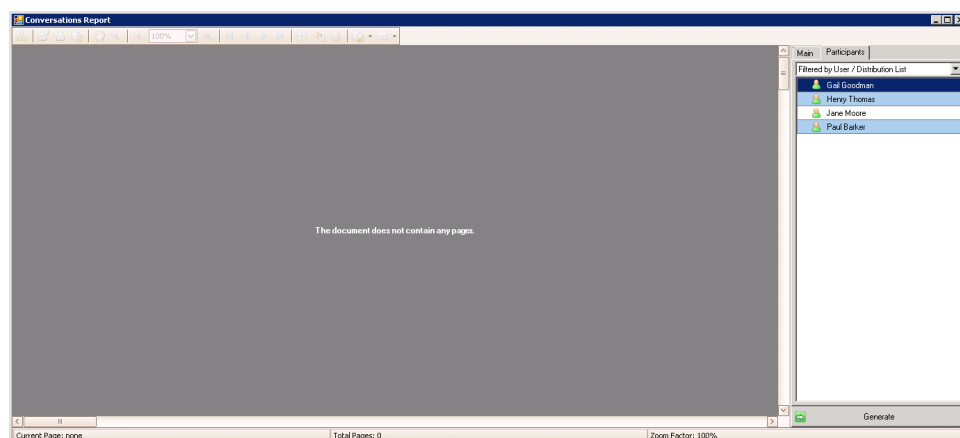


2. In the Reports pane, click **Conversations**. The Conversations Report window opens.

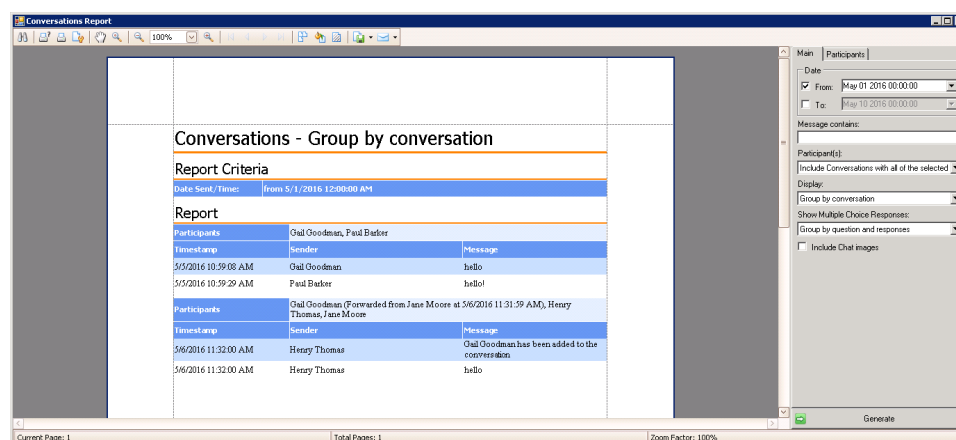


3. Click the **Participants** tab.

4. From the dropdown list that appears, select **All** to show all conversations, or select **Filtered by User / Distribution List** to specify the users whose conversations are to be displayed.
 - a. If you have selected **Filtered by User / Distribution List**, a list of users is displayed. Select the users whose conversations are to appear in the report.



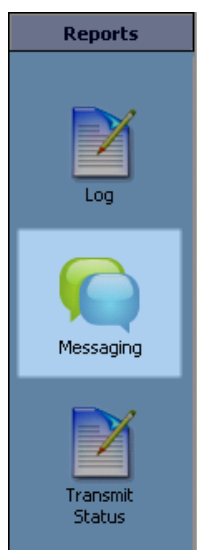
5. Click the **Main** tab.
6. In the **Date** section, in the **From** field, select the start date for which conversations are to be displayed. The default is midnight at the start of today's date.
7. In the **To** field, select the end date for conversations. The default is midnight at the start of the next day's date.
8. In the **Message contains** field, optionally type search criteria. If you specify any search criteria, only conversations that contain the search text are displayed.
9. From the **Participant(s)** dropdown list, select one of the following:
 - Include Conversations with all of the selected participants
 - Include Conversations with at least one selected participant
 These are the participants that you selected in the **Participants** tab.
10. From the **Display** dropdown list, select how the displayed conversations are to be organized. Select either **Group by conversation** or **Sort by timestamp**.
11. From the **Show Multiple Choice Responses** dropdown list, select how multiple choice responses are to be displayed. Select either **Group by question and responses** or **As part of conversation**.
12. Select the **Include Chat images** checkbox to include images sent in a conversation as part of the conversation report.
13. Click **Generate** to generate the conversations report.



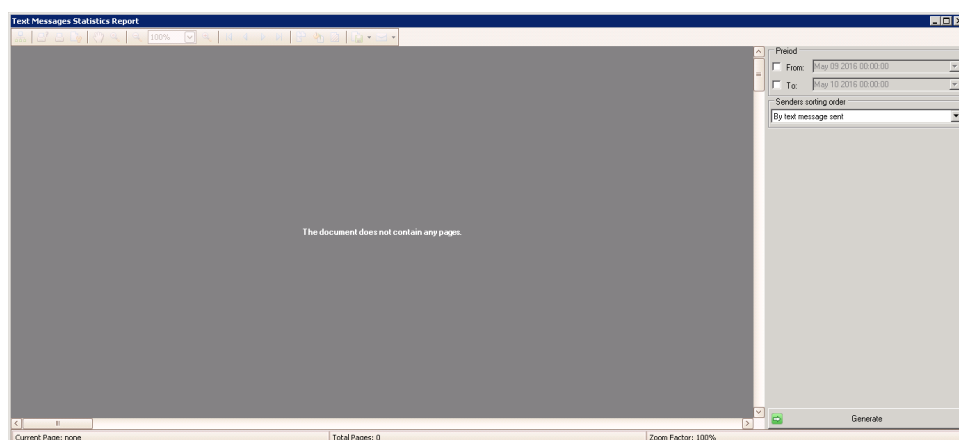
Creating a Text Messages Statistics Report

You can generate a report that provides details on the conversations or text messages for any user or group of users.

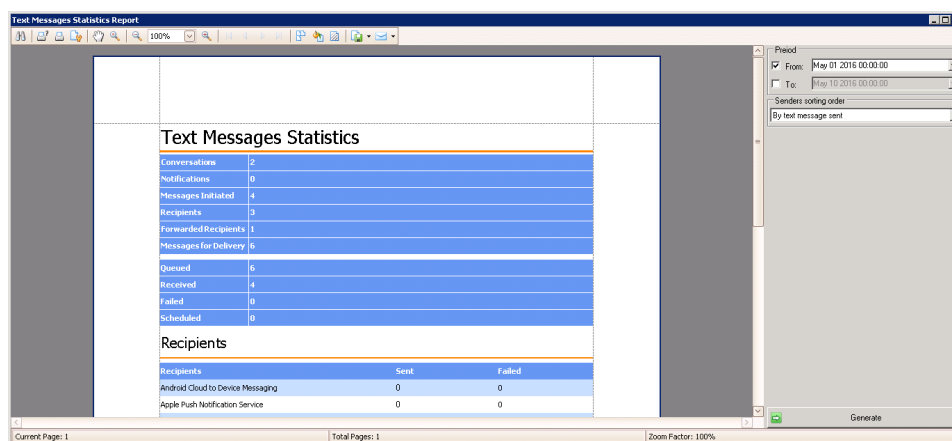
1. Open the VMP Administrator application and select **Reports > Messaging**.



2. In the Reports pane, click **Text Messages Statistics**. The Text Messages Statistics Report window opens.



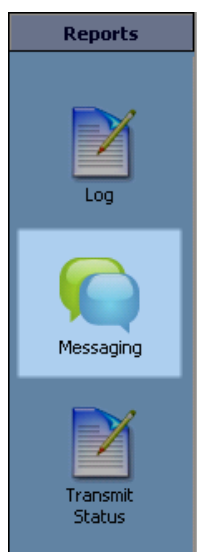
3. In the **Period** section, in the **From** field, select the start date for which conversations are to be displayed. The default is midnight at the start of today's date.
4. In the **To** field, select the end date for conversations. The default is midnight at the start of the next day's date.
5. From the **Senders sorting order** dropdown list, select how the displayed conversations are to be organized. Select either **By text message sent** or **By name**.
6. Click **Generate** to generate the text messages statistics report.



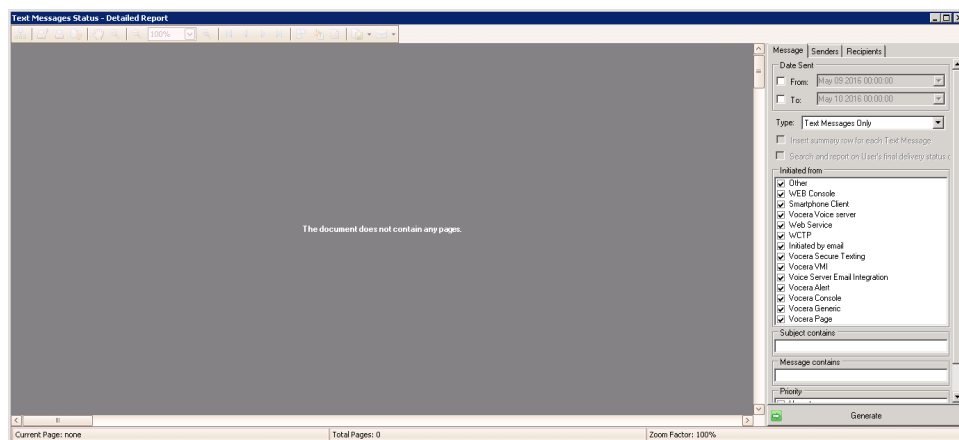
Creating a Detailed Text Messages Status Report

You can generate a report that provides detailed data on the text messages and status reports sent and received by the VMP Server. In this report, you can specify the message sources, senders, recipients, priority, and subject or message content.

1. Open the VMP Administrator application and select **Reports > Messaging**.

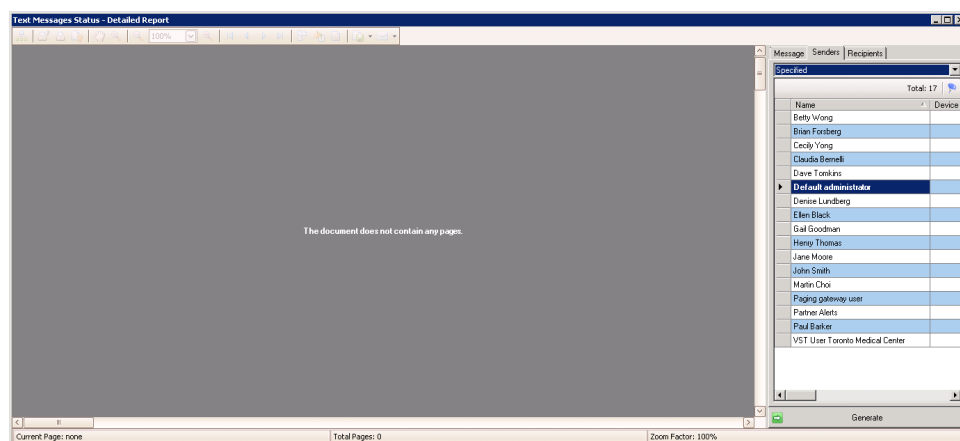


2. In the Reports pane, click **Text Messages Status - Detailed**. The Conversations Report window opens.

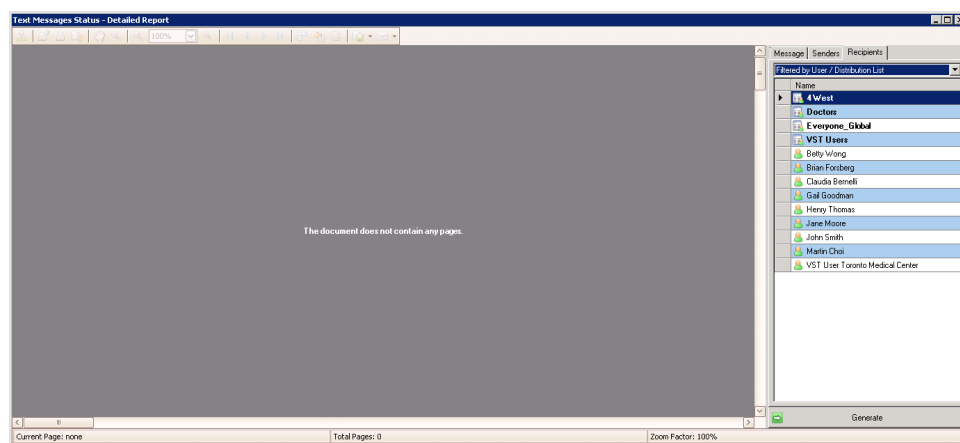


3. Click the **Message** tab.

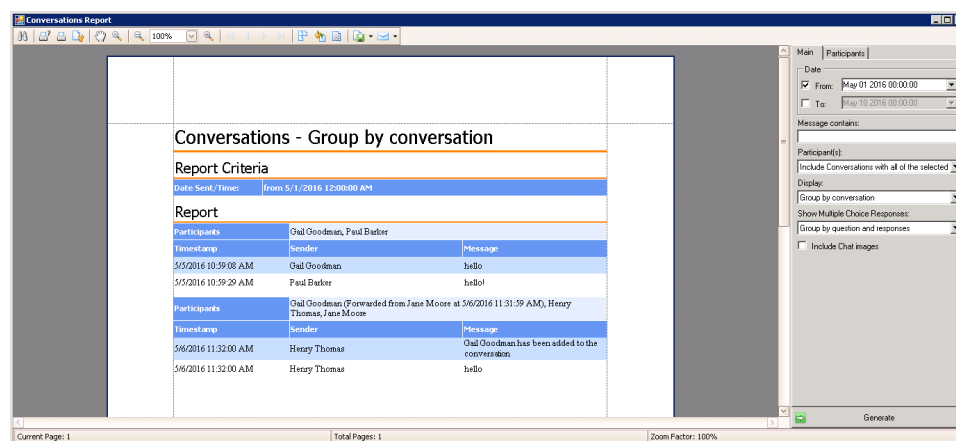
4. In the **Date Sent** section, in the **From** field, select the start date for which conversations are to be displayed. The default is midnight at the start of today's date.
5. In the **To** field, select the end date for conversations. The default is midnight at the start of the next day's date.
6. From the **Type** dropdown list, select the information to display in the report. Select either **Text Messages Only** or **Text Messages and Statuses**.
7. If you have selected **Text Messages and Statuses**:
 - a. Select the **Insert summary row for each Text Message** checkbox if you want the report to contain summary rows.
 - b. If needed, select the **Search and report on User's final delivery status only** check box.
8. In the **Initiated from** section, clear the checkboxes next to the message sources that you do not want to display in the report.
9. In the **Subject contains** field, optionally type search criteria. If you specify any search criteria, only conversations whose subject contains the search text are displayed.
10. In the **Message contains** field, optionally type search criteria. If you specify any search criteria, only conversations whose message body contains the search text are displayed.
11. In the **Priority** section, clear the checkboxes of the message priorities that you do not want to see in the report.
12. If you have selected **Text Messages and Statuses** from the **Type** dropdown list, the **Status** area appears, which displays the message statuses that you can include in the report. Clear the checkboxes of the message statuses that you do not want to see in the report.
13. Click the **Senders** tab.
14. From the dropdown list that appears, select **All** to show all senders, or select **Specified** to specify the senders whose conversations are to be displayed.
 - a. If you have selected **Specified**, a list of senders is displayed. Select the senders that are to appear in the report.



15. Click the **Recipients** tab.
16. From the dropdown list that appears, select **All** to show all recipients, or select **Filtered by User / Distribution List** to specify the recipients whose conversations are to be displayed.
 - a. If you have selected **Filtered by User / Distribution List**, a list of recipients is displayed. Select the recipients whose conversations are to appear in the report.



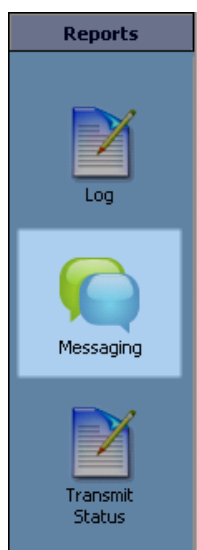
17. Click Generate to generate the detailed text messages status report.



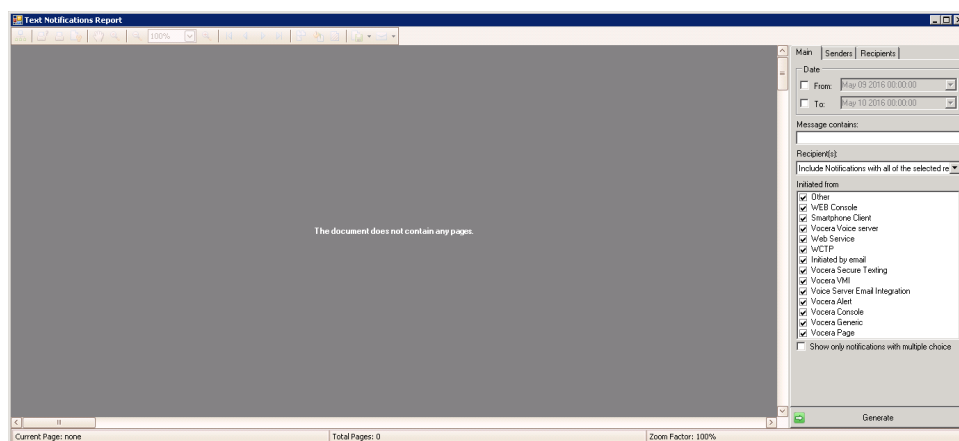
Creating a Text Notifications Report

You can generate a report that displays the text notifications sent and received in the VMP Server.

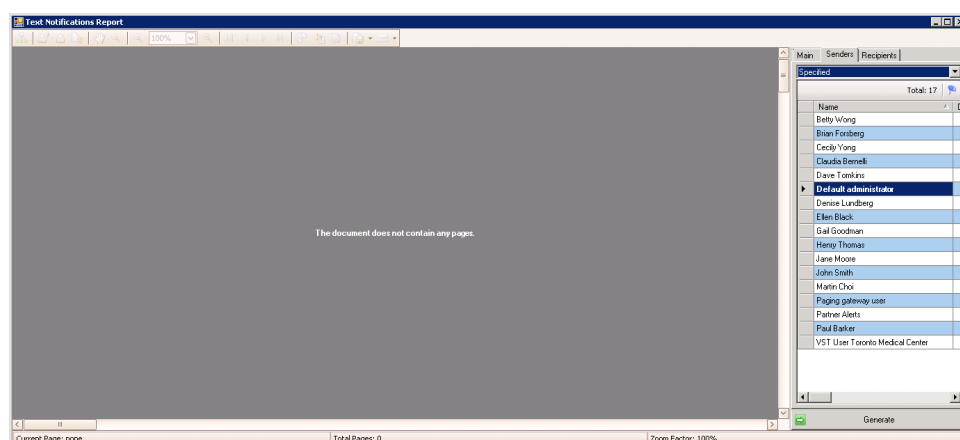
1. Open the VMP Administrator application and select Reports > Messaging.



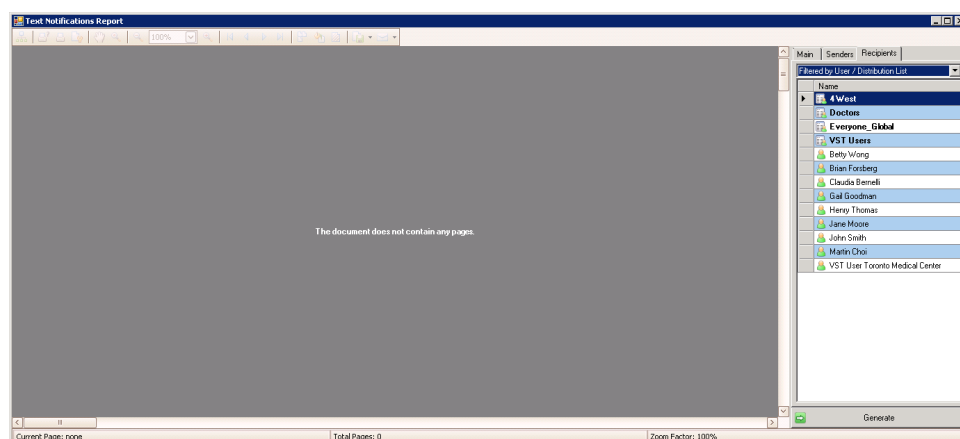
2. In the Reports pane, click Text Notifications. The Text Notifications Report window opens.



3. Click the Senders tab.
4. From the dropdown list that appears, select All to show all notifications, or select Specified to specify the senders whose notifications are to be displayed.
 - a. If you have selected Specified, a list of senders is displayed. Select the senders whose notifications are to appear in the report.

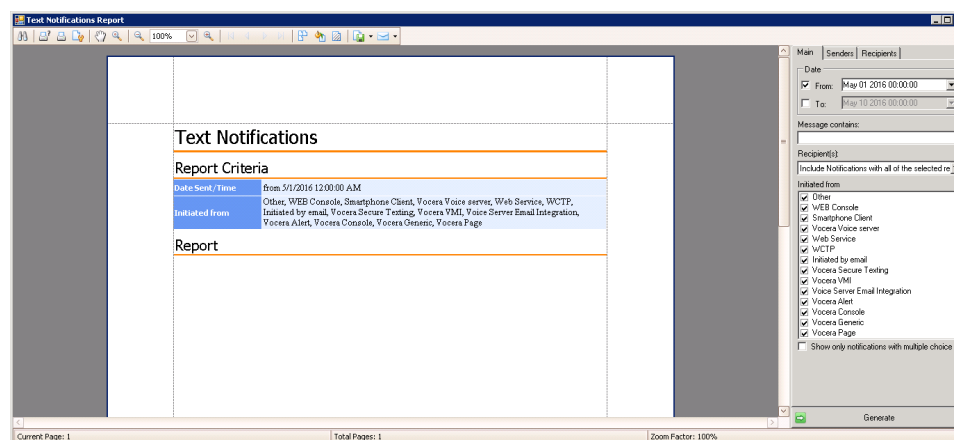


5. Click the Recipients tab.
6. From the dropdown list that appears, select All to show all notifications, or select Filtered by User / Distribution List to specify the recipients whose notifications are to be displayed.
 - a. If you have selected Filtered by User / Distribution List, a list of recipients is displayed. Select the recipients whose notifications are to appear in the report.



7. Click the Main tab.
8. In the Date section, in the From field, select the start date for which notifications are to be displayed. The default is midnight at the start of today's date.

9. In the To field, select the end date for notifications. The default is midnight at the start of the next day's date.
10. In the Message contains field, optionally type search criteria. If you specify any search criteria, only notifications containing the search text are displayed.
11. From the Recipient(s) dropdown list, select one of the following:
 - Include Notifications with all of the selected recipients
 - Include Notifications with at least one selected recipient
 These are the recipients that you selected in the Recipients tab.
12. In the Initiated from section, clear the checkboxes next to the message sources that you do not want to display in the report.
13. Select the Show only notifications with multiple choice responses checkbox to display only notifications for which a multiple choice response was requested.
14. Click Generate to generate the text notifications report.



About Transmit Status Reports

In the Reports module, you can display reports that list the status of Chat messages and content sent from the VMP Server.

Select the Transmit Status icon to display these reports.

The following Transmit Status reports can be generated:

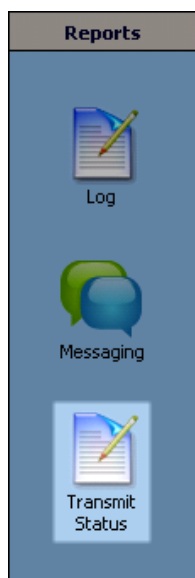
Table 31: Transmit Status reports

Report Type	Description
Chat by user - Legacy	For clients that have used the legacy Chat capability that was provided in previous versions of VMP, this displays transmit status information on Chat messages. You can specify the user for which Chat status information is to be displayed.
Content	Displays transmit status information on content transmitted from this server.

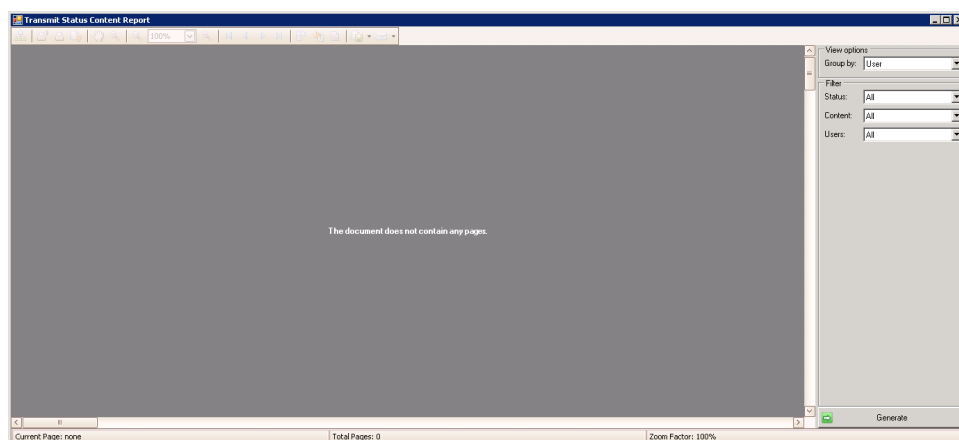
Creating a Content Transmit Status Report

You can generate a report that lists the users that have received content that has been provided for them.

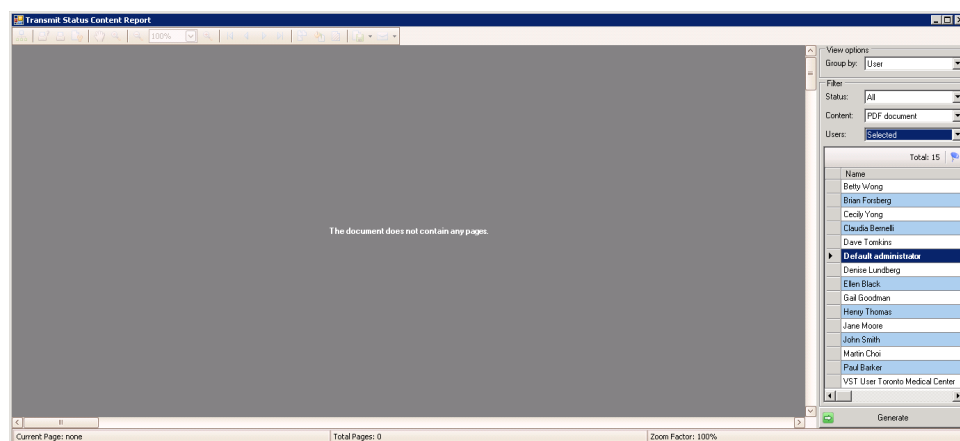
1. Open the VMP Administrator application and select Reports > Transmit Status.



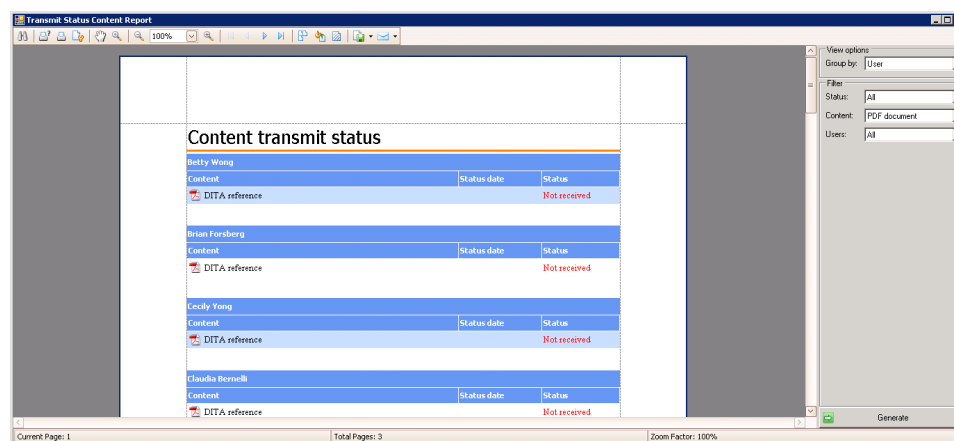
2. In the Reports pane, click Content. The Transmit Status Content Report window opens.



3. From the Group by dropdown list, select User to organize the report by user name, or select Content to organize the report by content items.
4. From the Status dropdown list, select one of the following:
 - All: Display all users, whether or not they have received the content.
 - Received: Display users that have received the content.
 - Not received: Display users that have not received the content.
5. From the Content dropdown list, select the type of content for which content transmit status information is to be displayed, or select All to display information for all content types.
6. From the Users dropdown list, select All to display content transmit status information for all users, or select Selected to specify the users for which you want to display information.
 - a. If you select Selected, a list of users appears. Select the user for which you want to display content transit status information.



7. Click Generate to generate the content transmit status report.



About Editing Reports










After you have created a report, you can use the tools provided to edit, print, or export the report.

These tools are available in a toolbar at the top of the report:



The following table describes these tools.

Tool	Description
Search	Search for a word or text in the report.
Print	Select a printer and print the report.
Print Direct	Print the report on the last selected printer.
Page Setup	Set up the report pages for printing.
Hand Tool	Move around in the displayed report.
Magnifier	Toggle between smaller and larger display views.
Zoom Out	Display more of the report in a smaller size.
Zoom	Specify the percentage size to use when displaying the report.
Zoom In	Display less of the report in a larger size.

Tool	Description
 First Page	Go to the first page of the report. This appears only when you are not already on the first page of the report.
 Previous Page	Go to the previous page. This appears only when you are not already on the first page of the report.
 Next Page	Go to the next page. This appears only when you are not already on the last page of the report.
 Last Page	Go to the last page of the report. This appears only when you are not already on the last page of the report.
 Multiple Pages	Display multiple pages at once.
 Background Color	Select the background color for the report.
 Watermark	Supply a watermark for each page of your report.
 Export Document	Export the document in the format specified in the dropdown menu. Depending on the format you specify, additional formatting options may appear.
 Send E-mail	Include the document in an email message in the format specified in the dropdown menu. Depending on the format you specify, additional formatting options may appear.

Configuration

The Configuration module enables you to customize your VMP environment to suit your needs.

The Configuration module is organized into views, which are listed in the table below.

Table 32: Configuration module views

View	Description
System Options	Manage system options.
Wireless Gateways	Create and modify system wireless gateways.
Contact Fields	Customize contact fields for your deployment.
Contact Source Mapping	Map contact fields to source fields.
User Source Mapping	Map user fields to source fields.
Plugin Configuration	Configure integrated plugins.
Licensed Applications	Manage application licensing.

For more information on System Options, see [VMP Administrator Configuration Options](#) on page 245. For more information on Wireless Gateways, see [Wireless Gateway Configuration](#) on page 99.

System Options

The System Options control the behavior of the VMP Server and the VMP Administrator.

For more information on system options, see [VMP Administrator Configuration Options](#) on page 245.

About Contact Fields

The [Contact Fields](#) module provides options to define the field source mapping appropriate for your contacts.

Field source mappings should be defined before the source import is initiated. You can map contact fields from one or many sources. This view also provides options to define field types specific for your environment.

Name	Type
Personal Photo	Photo
BlackBerry PIN	PIN
Email	Email
Photo	Image
Image 1	Image
Image 2	Image
Image 3	Image
Image 4	Image
Title	Text
Web Page	URL
Email 2	Email
Mobile Phone	Phone
Pager	Phone
Callback Phone	Phone

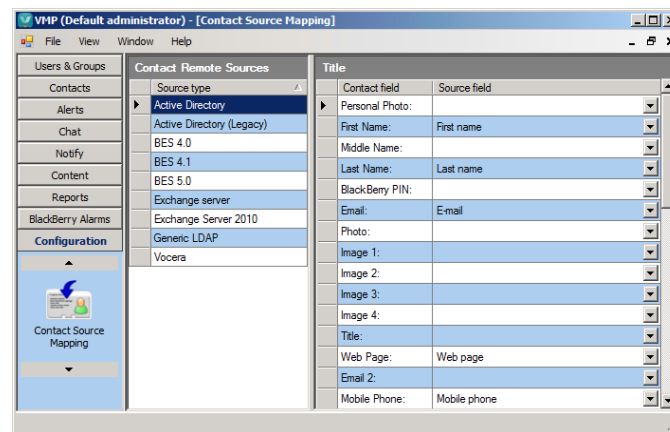
The Contact Fields view includes the following options:

Table 33: Contact field options

Option	Description
	Open the Define Field dialog to create a new field.
	Delete a highlighted field.
	Edit a highlighted field.
	Move the highlighted field up.
	Move the highlighted field down.
	Define the fields that are included in a search from the client for indexing.

About Contact Fields

Use the VMP Administrator Contact Source Mapping module to edit contact fields.



This view lists available sources on the left. Click to highlight the source for mapping edits. Each source field is listed on the right. The fields contain a dropdown list to map the source field to a VMP field.



Tip: The field mappings are also defined during an initial source import. Use this view only when updates are required.

About User Field Editing

Use the VMP Administrator User Source Mapping module to map VMP fields to fields from the import source.

This view lists available sources on the left. Click to highlight the source for mapping edits. Each source field is listed on the right. The fields contain a dropdown list to map the source field to a VMP field.



Tip: The field mappings are also defined during an initial source import. Use this view only when updates are required.


Plugin Configuration

Use the Plugin configuration view to add and configure licensed plugins for your deployment.

The following plugin configurations are supported.

Table 34: Plugin configuration support

Plugin	Settings
MIR3 Voice	Enter the following settings: <ul style="list-style-type: none"> • URL • Username • Password • Confirm Password
SendWordNow Voice	Enter the following settings: <ul style="list-style-type: none"> • Login • Password • Confirm Password
TFC Voice	Enter the following settings: <ul style="list-style-type: none"> • Username • Password • Confirm Password • cli_id • user_id • caller_id
Voice Gate	Enter the following settings: <ul style="list-style-type: none"> • Client Name • Client ID • Confirm Client ID • Display Number

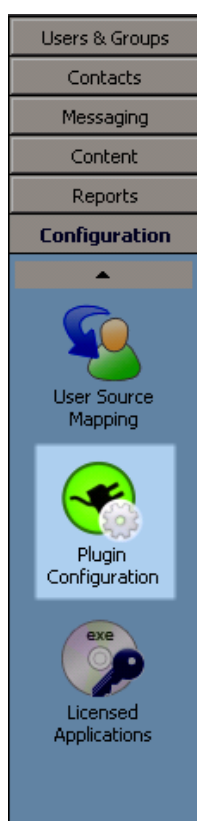
Plugin	Settings
GE MUSE integration	<p>Enter the following settings:</p> <ul style="list-style-type: none"> Scanning folder (Required field): The local or network location where incoming GE MUSE XML files will be located. The service account credentials used by the Vocera Data Exchange service are used to authenticate to network locations. XML Mapping Field (Required field): The XML tag to use when mapping field values to Distribution Lists. Examples of commonly used XML tags include <ReferringMDLastName> and <SiteName>. <p> Note: The value of this field - the XML tag to match in incoming messages - is referred to as XMLMappingField elsewhere in this section.</p> <ul style="list-style-type: none"> Default distribution list (Required field): Used if the defined Mappings do not match the value of XMLMappingField that is specified in the incoming XML. Default notification distribution list (Required field): When a new XML file is processed for an unmatched XMLMappingField value, send a notification to this Distribution List. Mapping 1 through Mapping 40 (Optional fields): Enter XMLMappingField = <Distribution List Name> to map each XMLMappingField value specified in the incoming XML to its corresponding Distribution List name. Notification DL 1 through Notification DL 40 (Optional fields): When a new XML file is processed that matches the specified Mapping, send a notification to this Distribution List. <p>The body of a generated message contains the following fields from the GE MUSE XML file:</p> <p>Subject: GE MUSE consult from XMLMappingField Patient ID: <PatientID> Patient Name: <PatientLastName>, <PatientFirstName> Gender: <Gender> Age: <PatientAge> Ordering Physician: <HISOrderingMDLastName>, <HISOrderingMDFirstName> <TestReason></p> <p>All messages are given Urgent priority. When a new XML file is processed, the format for the notification sent to the notification Distribution List is:</p> <p>Subject: GE MUSE consult status changed for Patient ID <PatientID> at XMLMappingField MappingFieldValue Body: The GE MUSE consult request sent to <first name> <last name> received the response <response> at <timestamp>.</p>
MIR3 SMS	<p>Enter the following settings:</p> <ul style="list-style-type: none"> URL Username Password Confirm Password
SendWordNow SMS connector	<p>Enter the following settings:</p> <ul style="list-style-type: none"> Login Password Confirm Password
SMTP connector	<p>Enter the following settings:</p> <ul style="list-style-type: none"> Server Port SSL PrimaryPagerID

Plugin	Settings
MIR3 FAX	Enter the following settings: <ul style="list-style-type: none"> • Company • URL • Username • Password • Confirm Password
WIC PIN Blaster	Enter the following settings: <ul style="list-style-type: none"> • Server • Login • Password • Confirm Password

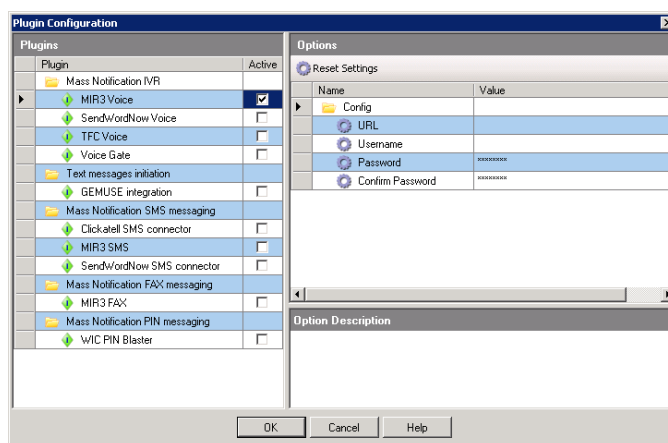
Using the Plugin Configuration Module

You can configure any licensed plugin that you have added to your VMP Server.

1. From the VMP Administrator, select **Configuration > Plugin Configuration**.



2. Click the **Active** checkbox for the plugin you want to configure.





3. For each required setting, enter its value in the *Value* column.
4. Click **OK** to save the configuration.

Licensed Applications

Use the Vocera Messaging Platform Licensed Application view to display available application licenses and assign licenses to platform users. This view lists each licensed application, the available licenses, and the number of licenses currently assigned to users.

To display the Licensed Application view, select **Configuration > Licensed Applications**.



Highlight an application to view the assigned users. Add or remove a licensed user from an application by clicking to highlight the user and selecting **Add**  or **Delete** .

Licensed Applications				Users		
Name	Total	In Use	Assigned	Name	Device ID	Email
Chat	25100	0	3	Total: 3		
Contacts	25100	0	3	Brian Forsberg		bforsberg@dhll.loc
Content	25100	0	2	Gail Goodman		ggoodman@dhll.loc
Alert	25100	0	3	Henry Thomas		hthomas@dhll.loc
Alert(SNPP/WCT...	25100	0	0			

The VMP Web Console

The VMP Web Console provides a browser-based way to send messages, view on-call status, and create schedules. You can also place calls from the VMP Web Console if your device is logged into Vocera Collaboration Suite.

VMP Web Console Overview

The VMP Web Console provides administrator and user access to the VMP communication platform from your Web browser.

The URL for the VMP Web Console is the DNS entry or the IP address of the VMP Server.

Depending upon the firewall configuration, the VMP Web Console can be opened up to external, off-network users.

Users are assigned access to the VMP Web Console in the VMP Administrator. For details about granting users access to the VMP Web Console, see [Granting Existing Users Access to the VMP Web Console](#) on page 222.

Browser Requirements

The VMP Web Console is supported on Internet Explorer version 10 and 11.

Logging into the VMP Web Console

To use the VMP Web Console, you must log in.

The screenshot shows the Vocera Web Console login interface. At the top left is the Vocera logo, and at the top right is the text 'Web Console'. The main heading is 'Log in to Vocera'. Below this are two input fields: 'Username' with a person icon and 'Password' with a magnifying glass icon. An orange 'Log in' button is positioned below the password field. At the bottom left, it says '© 2017 Vocera', and at the bottom right, there is a 'HELP' link.

1. In the Username field, type your username.
2. In the Password field, type the password for your username.
3. Click Log in to log in to the VMP Web Console.

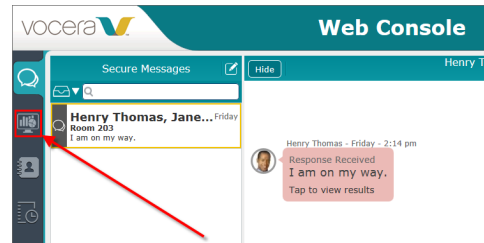


Note: If you are a Vocera Secure Texting user, you cannot log into the VMP Web Console.

The Monitor View

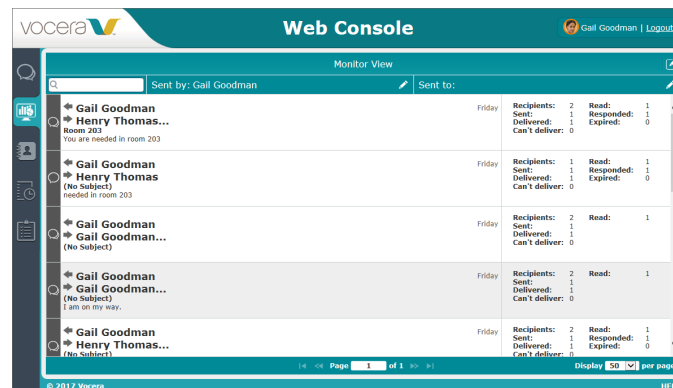
The VMP Web Console Monitor View lists messages sent or received by the users for which you have granted viewing permission.

To access the Monitor view, select the Monitor View icon.



Note: This icon appears only when the user that is logged on has permission to view either sent messages or received messages. See [Allowing Users to View Messages](#) on page 226 for more information on granting permission to view messages.

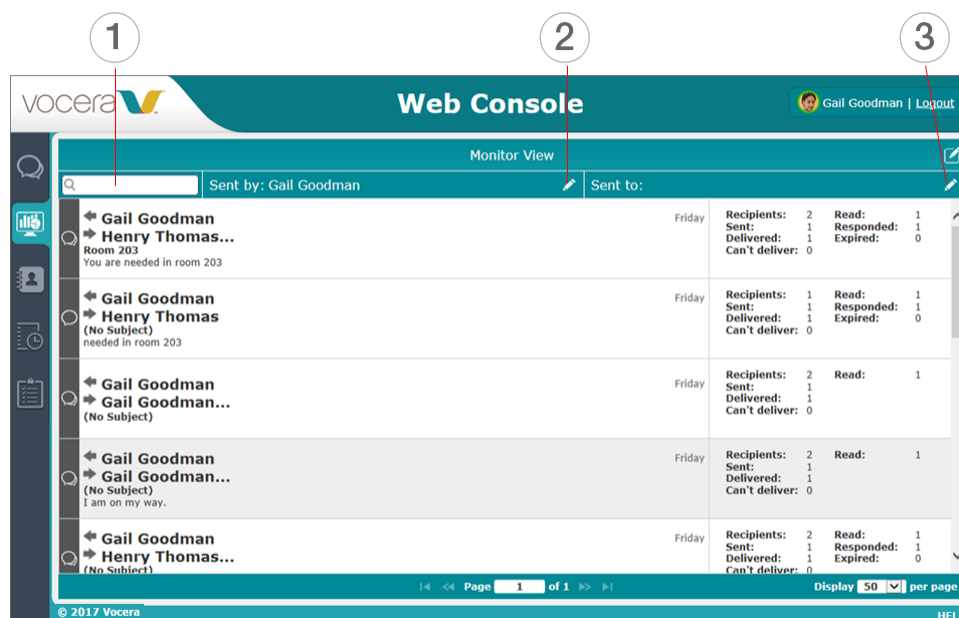
The Monitor View lists each message.



Click a message to display its details.

Monitor View Features

From the Monitor View, you can search for messages, or select the source or recipient of a message.



- 1 Use the search box to search for messages by:
 - Sender
 - Recipient
 - Subject
 - Keyword (in the message subject)
- 2 The Sent by field. Click the pencil icon to create Sent By filters.
- 3 The Sent to field. Click the pencil icon to create Sent To filters.

For more information on using the Sent By and Sent To filters, see [Filtering the Monitor View](#) on page 194.



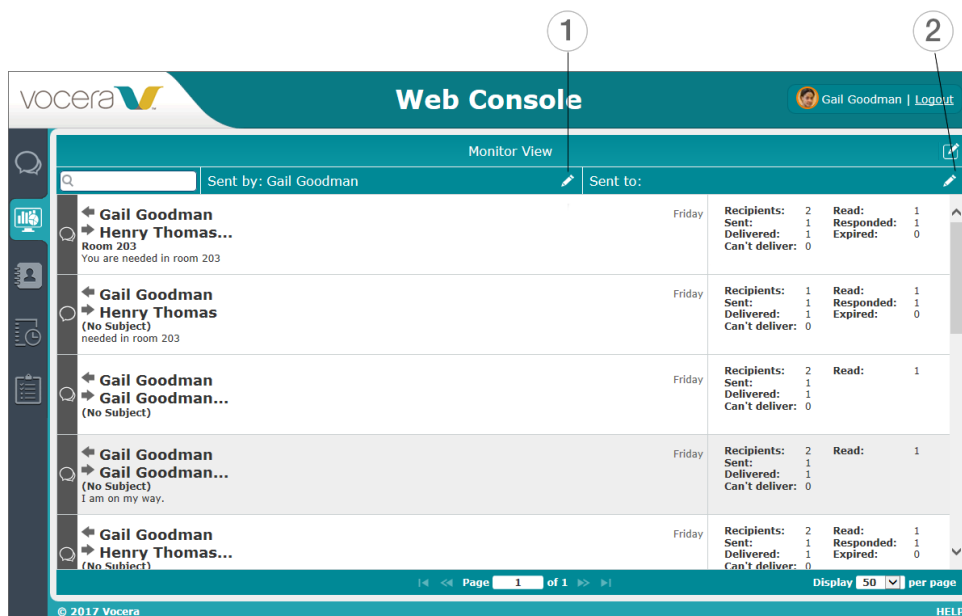
Note: You must use the VMP Administrator to grant permission for a user to view messages sent or received by any other user. See [Allowing Users to View Messages](#) on page 226 for more information on granting permission to view messages.

Filtering the Monitor View

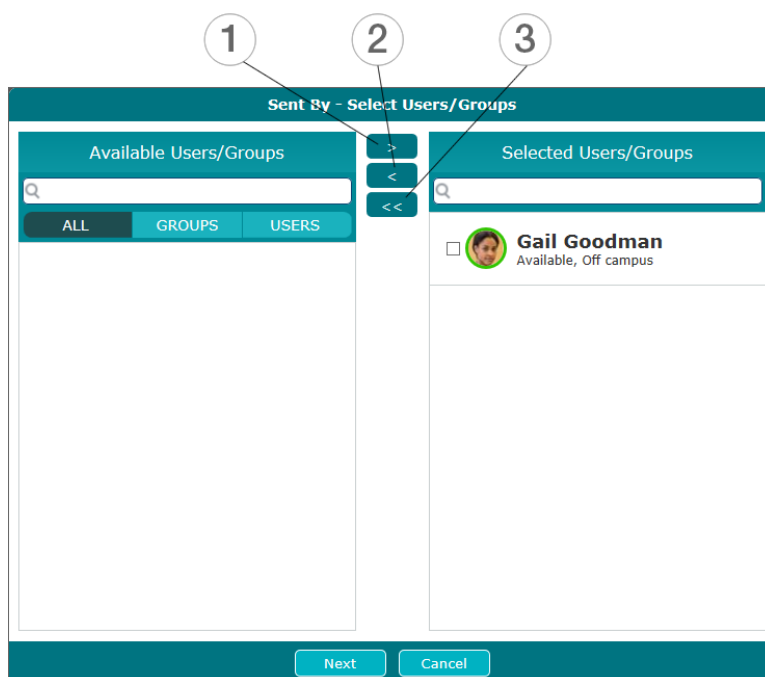
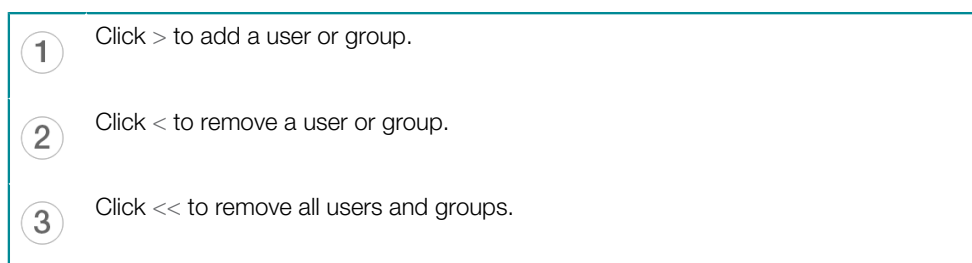
In the Monitor View, you can create Sent By and Sent To filters that limit the messages that are displayed on the screen.

1. Do one of the following:

- 1 Click the pencil icon in the Sent by field to edit the Sent By filter.
- 2 Click the pencil icon in the Sent to field to edit the Sent To filter.



2. In the Select Users/Groups dialog box, select the All tab to display both users and groups, select the Groups tab to display groups only, or select Users to display users only.
3. Select the checkboxes of the users and groups to include in the filter:



4. Click Next.

- In the selection tree dialog box that appears, select the checkboxes of the criteria to be matched for messages to appear in the Monitor View. You can select separate criteria for secure messages and for notifications.

The screenshot shows a dialog box titled "Sent By - Select Users/Groups". It is divided into two main sections: "Secure Messages" on the left and "Notifications" on the right. Each section contains a tree of criteria with checkboxes. Under "Secure Messages", the criteria are: "Responses" (checked), "Expiration" (checked), and "Priority" (checked). Under "Responses", "With Responses" and "Without Responses" are both checked. Under "Expiration", "Expired", "Not Expired", and "Does not have Expiration" are all checked. Under "Priority", "Normal", "High", and "Urgent" are all checked. The "Notifications" section has an identical set of criteria, all of which are also checked. At the bottom of the dialog are three buttons: "Back", "Save", and "Cancel".

- Click **Save** to save this filter, or click **Cancel** to cancel editing the filter. Click **Back** to return to selecting users and groups.

Web Console Secure Messages

Vocera Messaging Platform users can create or send a secure message to users or Distribution Lists using the VMP Web Console. The console provides an interface for sending messages from your Web browser.

You can grant access to the VMP Web Console when you create, import, or edit users. Users can create messages from existing templates if they have been made available, and they can edit the templates if you enable that option.



Note: The text of a message can be up to 3000 characters long, and the subject header can contain up to 512 characters. Any ASCII character can be included, but emojis are not supported.

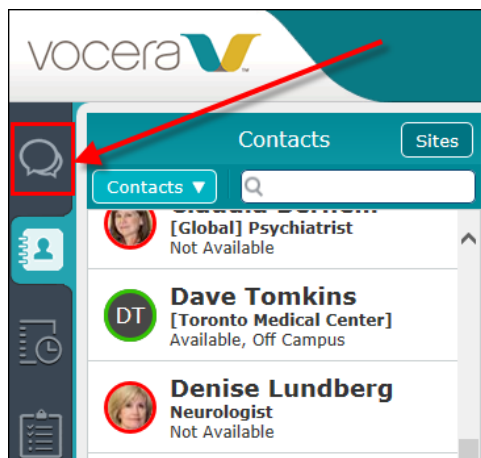
Sending a Message from the VMP Web Console

You can use the VMP Web Console to send a message to any user or Distribution List.

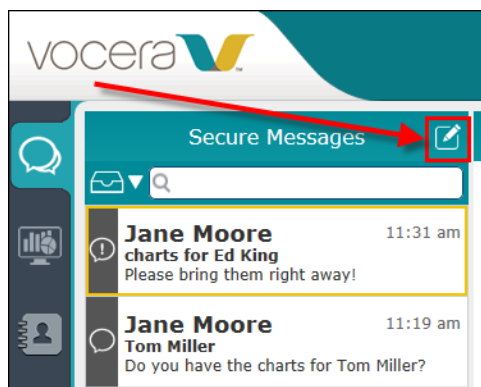


Note: If the message has more than 50 recipients, it is defined to be a Mass Notification. See [About Mass Notifications](#) on page 208 for details.

- Open the VMP Web Console from your Web browser.
- Select the **Message** tab.



3. Click the Compose icon.



The New Secure Message screen appears.

4. Select New Text to create a new message.



You can also create a message using a message template. This enables you to send an emergency message quickly. For information on how to send a message using a template, see [Sending a Message Using a Template](#) on page 200.

5. To add one or more message recipients, either type the recipient name in the To: field, or click the Add Recipient icon to select a Distribution List or user to add to the recipient list.

Web Console Gail Goodman | Logout

New Secure Message

To:

Subject:

[Click to attach patient info](#)



Note: If a recipient is having messages forwarded to another contact, that contact is automatically added to the list of recipients when the message is sent.

6. If you have clicked the Add Recipient icon, the Select Recipients dialog box appears. Select the Favorites tab to display favorites only, or select the Contacts tab to display all contacts.



Note: See [Using Web Console Favorites](#) on page 239 for more information on creating favorites.

7. Select the checkboxes of the users and Distribution Lists to include as recipients:

- 1 Click > to add a recipient.
- 2 Click < to remove a recipient.
- 3 Click << to remove all recipients.

Select Recipients

Available Users

Selected Users

FAVORITES CONTACTS

Brian Forsberg
[Global] Family Physician
Not Available

Cecily Yong
[Toronto Medical Center] Mana...
Available, Off Campus

Claudia Bernelli
[Global] Psychiatrist
Not Available

Dave Tomkins
[Toronto Medical Center]
Available, Off Campus

OK Cancel

8. If your message has a subject, type the subject text in the Subject field.
9. To attach patient information to this message:
- a. Click the Click to attach patient info link. The Select Patient dialog box appears:

Select Patient

Search by name, room, unit or MRN

MY PATIENTS ALL PATIENTS

Ismael Q. Abel
Room: 7063 DoB: Jan/09/1954
Unit: HATH 07PP
MRN: IsmaelAbel19540109

GABRIEL ACUNA
Room: CC473 DoB: Jun/14/1984
Unit: FACILITY CARDIO
MRN: 12345640202275565

Eugene Y. Adair
Room: 12030 DoB: Mar/14/1973
Unit: HATH 12Med
MRN: EugeneAdair19730314

BARBARA S ADAMS
Room: CC593 DoB: Dec/27/1945
Unit: FACILITY CARDIO
MRN: 1234564020180919

BARBARA S ADAMS
Room: N593 DoB: Dec/27/1945
Unit: FACILITY CARDIO

OK Cancel

If no patient information is available, this link does not appear.

- Click **My Patients** to view your patient list only, or click **All Patients** to view a list of all available patients.
- Type text in the search field to limit the patient list to patients whose name matches your search text.
- Select the patient whose information you want to attach to this message.
- Click **OK** to close the **Select Patient** dialog box. The message now contains a link to the patient information that you have selected.

vocera Web Console Gail Goodman | Logout

Cancel New Secure Text

To: Doctors

Subject:

BARBARA S ADAMS - Room: CC593 - DoB: Dec/27/1945 (71)

Priority Attach Media Responses Type your message here Send

© 2017 Vocera HELP

- Click **Priority** to specify a priority for the message. Select one of **Normal**, **High**, or **Urgent**. The following table lists the notifications sent for each priority:

Priority	Notifications in VCS app
Normal	Single ring and vibration
High	Multiple rings and vibrations
Urgent	Multiple rings (overriding user's volume setting) and vibrations



Important: On some devices, messages sent with Urgent priority may be spoken out loud to some recipients. Sending confidential patient health information with this priority may violate privacy regulations.

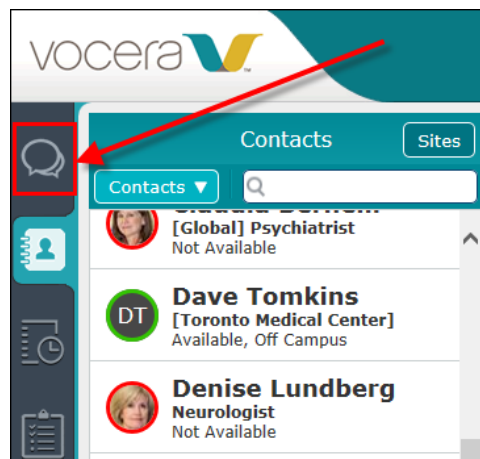
11. Do one of the following:
 - a. To send a text message, type the message text in the field at the bottom of the screen and click **Send**.
 - b. To send a photo, click **Attach Media** and select the image that you want to send.
 - c. To create a message that requires a response, click **Responses**. This displays the interface for sending a message that requires a response. See [Sending a Message That Requires a Response](#) on page 204 for more details.

Sending a Message Using a Template

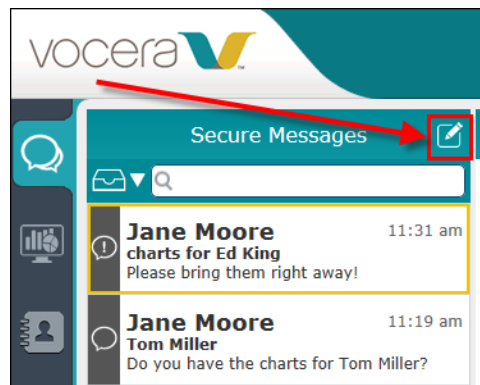
Message templates enable you to send emergency messages quickly, as the text and recipients are defined for you in the VMP Administrator.

For information about creating templates, see [Creating Messaging Templates](#) on page 144.

1. Open the VMP Web Console from your Web browser.
2. Select the **Message** tab.

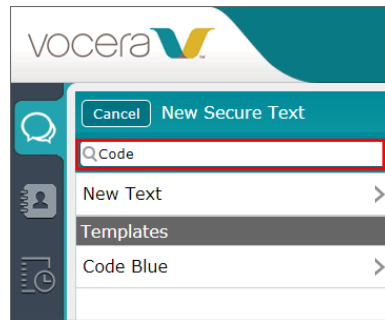


3. Click the **Compose** icon.

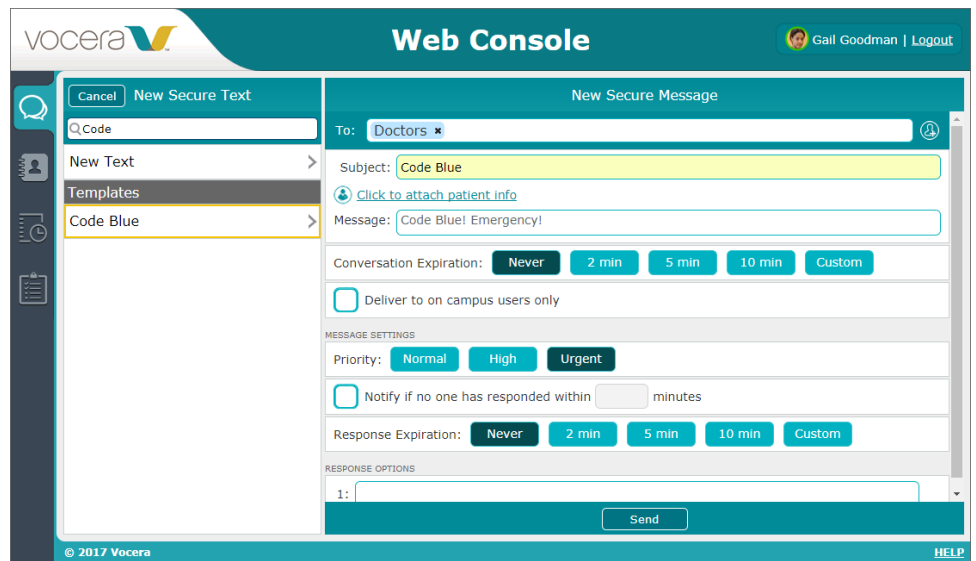


The New Secure Message screen appears.

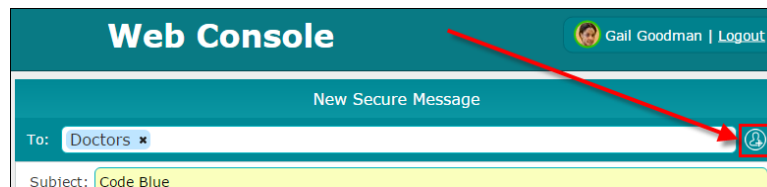
4. Select the message template from the list of templates. If you have defined a large number of templates, type text in the template search field to display only the templates that match your search text. If you are looking for a template with a long name, expand the New Secure Text pane to view it.



The message template appears.



5. Your template may already have specified default recipients for your message. To add one or more additional message recipients, either type the recipient name in the **To:** field, or click the Add Recipient icon to select a Distribution List or user recipient.



Note: If a recipient is having messages forwarded to another contact, that contact is automatically added to the list of recipients when the message is sent.

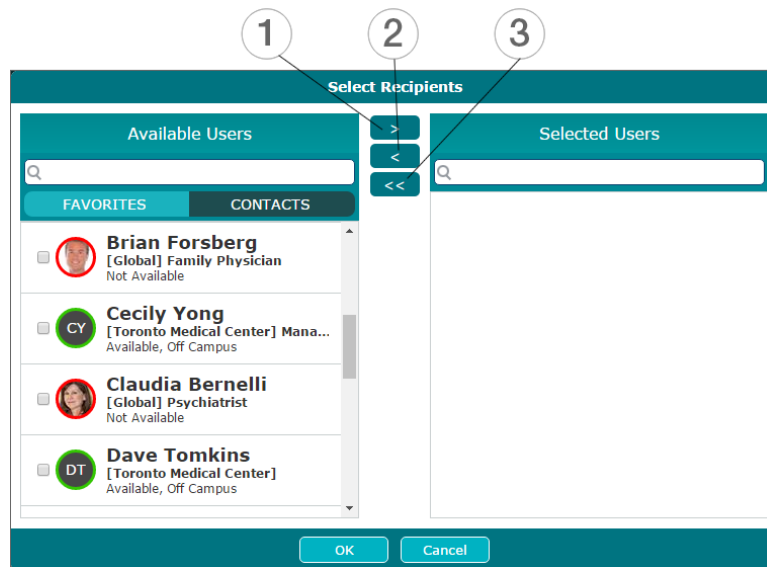
6. If you have clicked the Add Recipient icon, the Select Recipients dialog box appears. Select the Favorites tab to display favorites only, or select the Contacts tab to display all contacts.

Note: See [Using Web Console Favorites](#) on page 239 for more information on creating favorites.

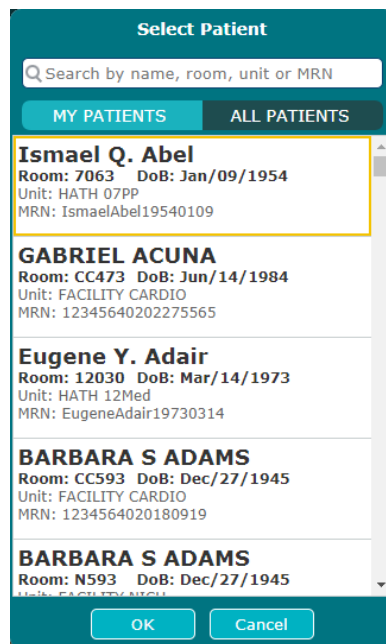
7. Select the checkboxes of the users and Distribution Lists to include as recipients:

- 1 Click > to add a recipient.
- 2 Click < to remove a recipient.

- 3 Click << to remove all recipients.



8. In the **Subject** field, type or edit the message subject if it is needed. The message template may have provided this text for you.
9. To attach patient information to this message:
 - a. Click the **Click to attach patient info** link. The **Select Patient** dialog box appears:



If no patient information is available, this link does not appear.

- b. Click **My Patients** to view your patient list only, or click **All Patients** to view a list of all available patients.
 - c. Type text in the search field to limit the patient list to patients whose name matches your search text.
 - d. Select the patient whose information you want to attach to this message.
 - e. Click **OK** to close the **Select Patient** dialog box.
10. In the **Message** field, type or edit the message text. The message template may have provided this text for you.



11. To specify an expiration time in minutes for your message, click one of the buttons in the Conversation Expiration row:

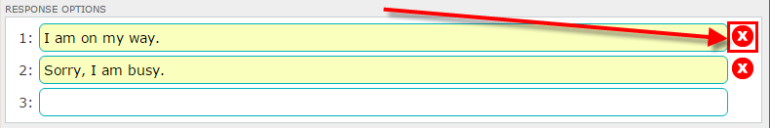
- Never, which indicates that the message never expires (this is the default setting)
- 2 min
- 5 min
- 10 min
- Custom

If you click Custom, a field appears in which you can specify the number of minutes before the message expires:

12. Select the Do not deliver to off campus users checkbox if this message is to be delivered only to users who are on-campus. This ensures that emergency messages are sent only to those people who can immediately respond to them.

13. Configure the following options.

Option	Description
Priority	<p>One of the following:</p> <ul style="list-style-type: none"> • Normal (the default) • High • Urgent <p>See Sending a Message from the VMP Web Console on page 196 for details on how these priority levels are handled in the VCS app.</p> <p> Important: On some devices, messages sent with High or Urgent priority may be spoken out loud to some recipients. Sending confidential patient health information with either of these priorities may violate privacy regulations.</p>
Notify if no one has responded	<p>Select this checkbox if you want to be notified when no one has responded within the number of minutes that you specify in the text field. If no one responds to this message during this time period, the Notify Me icon is displayed in the message link:</p> <p></p> <ul style="list-style-type: none"> • If you are logged onto a Vocera badge, the notification is sent as a message on the badge. • If you are logged into a badge and on to the Vocera Collaboration Suite, a tone notification is sent to the badge, and the Notify Me icon is displayed in the message link. • If you are logged into a badge and on to the VMP Web Console, a tone notification is sent to the badge, and the Notify Me icon is displayed in the message link.
Response Expiration	<p>Specify the time period, in minutes, in which responses to this message are allowed. This time period is indicated on the sent message. Select Custom to specify a time period.</p>

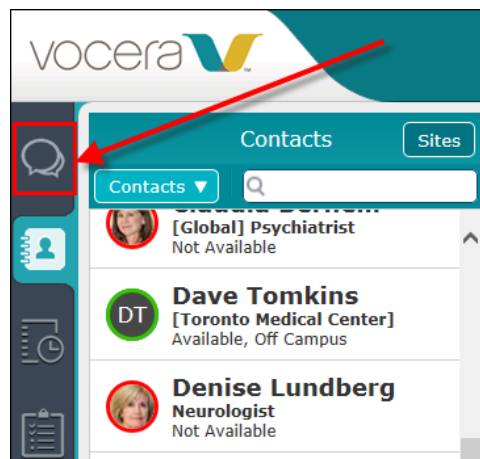
Option	Description
Response Options	<p>If the communication requires a response, set multiple choice options to help the recipient respond quickly. When you type an option, a new field appears to enable you to type an additional option if necessary. To delete an option that you have created, click the Delete icon:</p> 

- Click Send to send the message, or click Cancel to return to the message interface described in [Sending a Message from the VMP Web Console](#) on page 196.

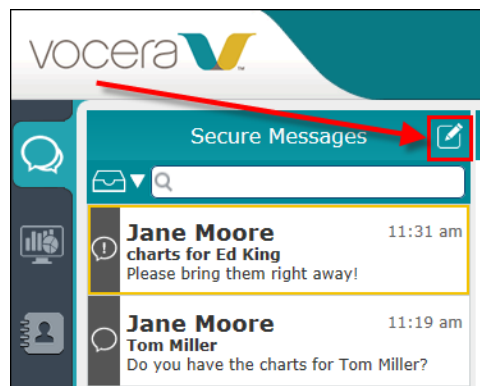
Sending a Message That Requires a Response

You can send a message that requires the recipient to provide a response.

- Open the VMP Web Console from your Web browser.
- Select the Message tab.



- Click the Compose icon.



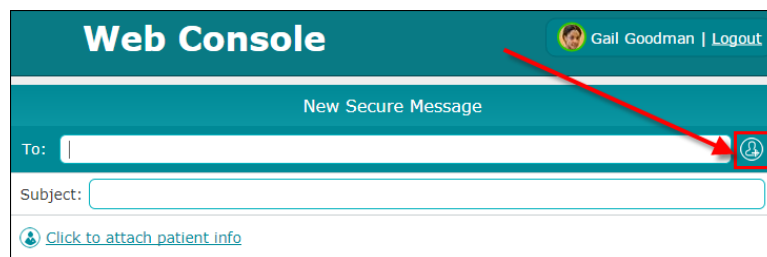
The New Secure Message screen appears.

- Select New Text to create a new message.



You can also create a message using a message template. This enables you to send an emergency message quickly. For information on how to send a message using a template, see [Sending a Message Using a Template](#) on page 200.

5. To add one or more message recipients, either type the recipient name in the To: field, or click the Add Recipient icon to select a Distribution List or user to add to the recipient list.



Note: If a recipient is having messages forwarded to another contact, that contact is automatically added to the list of recipients when the message is sent.

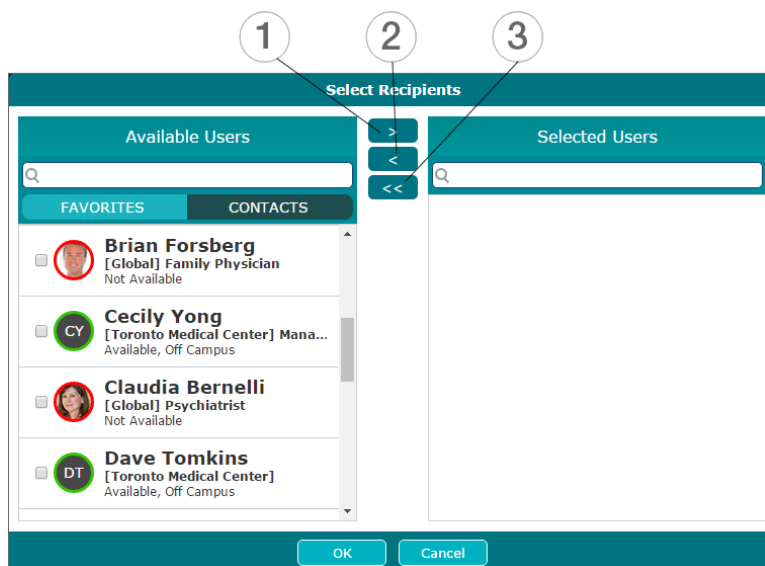
6. If you have clicked the Add Recipient icon, the Select Recipients dialog box appears. Select the Favorites tab to display favorites only, or select the Contacts tab to display all contacts.



Note: See [Using Web Console Favorites](#) on page 239 for more information on creating favorites.

7. Select the checkboxes of the users and Distribution Lists to include as recipients:

- 1 Click > to add a recipient.
- 2 Click < to remove a recipient.
- 3 Click << to remove all recipients.



8. Click Responses to display the screen for sending a message with a response.



9. In the Subject field, type an subject for the message if it is needed.
10. To attach patient information to this message:
- Click the Click to attach patient info link. The Select Patient dialog box appears:

Select Patient

Search by name, room, unit or MRN

MY PATIENTS ALL PATIENTS

Ismael Q. Abel
Room: 7063 DoB: Jan/09/1954
Unit: HATH 07PP
MRN: IsmaelAbel19540109

GABRIEL ACUNA
Room: CC473 DoB: Jun/14/1984
Unit: FACILITY CARDIO
MRN: 12345640202275565



Eugene Y. Adair
Room: 12030 DoB: Mar/14/1973
Unit: HATH 12Med
MRN: EugeneAdair19730314

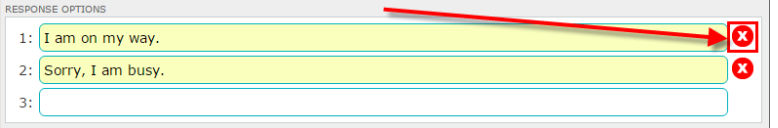
BARBARA S ADAMS
Room: CC593 DoB: Dec/27/1945
Unit: FACILITY CARDIO
MRN: 1234564020180919

BARBARA S ADAMS
Room: N593 DoB: Dec/27/1945
Unit: FACILITY CARDIO

OK Cancel

- b. Click My Patients to view your patient list only, or click All Patients to view a list of all available patients.
 - c. Type text in the search field to limit the patient list to patients whose name matches your search text.
 - d. Select the patient whose information you want to attach to this message.
 - e. Click OK to close the Select Patient dialog box.
11. In the Message field, type the text of the message.
 12. Configure the following options.

Option	Description
Priority	<p>One of the following:</p> <ul style="list-style-type: none"> Normal (the default) High Urgent <p>See Sending a Message from the VMP Web Console on page 196 for details on how these priority levels are handled in the VCS app.</p> <p> Important: On some devices, messages sent with Urgent priority may be spoken out loud to some recipients. Sending confidential patient health information with either of these priorities may violate privacy regulations.</p>
Notify if no one has responded	<p>Select this checkbox if you want to be notified when no one has responded within the number of minutes that you specify in the text field. If no one responds to this message during this time period, the Notify Me icon is displayed in the message link:</p> <p></p> <ul style="list-style-type: none"> If you are logged onto a Vocera badge, the notification is sent as a message on the badge. If you are logged into a badge and on to the Vocera Collaboration Suite, a tone notification is sent to the badge, and the Notify Me icon is displayed in the message link. If you are logged into a badge and on to the VMP Web Console, a tone notification is sent to the badge, and the Notify Me icon is displayed in the message link.
Response Expiration	<p>Specify the time period, in minutes, in which responses to this message are allowed. This time period is indicated on the sent message. Select Custom to specify a time period.</p>

Option	Description
Response Options	<p>If the communication requires a response, set multiple choice options to help the recipient respond quickly. When you type an option, a new field appears to enable you to type an additional option if necessary. To delete an option that you have created, click the Delete icon:</p> 

- Click **Send** to send the message, or click **Cancel** to return to the message interface described in [Sending a Message from the VMP Web Console](#) on page 196.

About Mass Notifications

When you create a message that has more than 50 recipients, it is automatically treated as a Mass Notification.

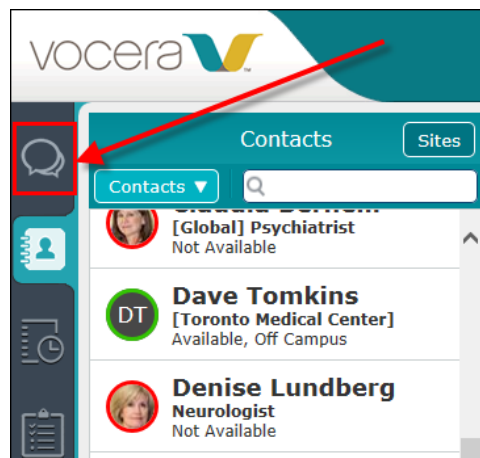
When you receive a Mass Notification, the text *N Participants* is shown as the recipient, where *N* is the number of recipients.

The list of Mass Notification recipients can be displayed in the VMP Web Console, but cannot be displayed on user devices.

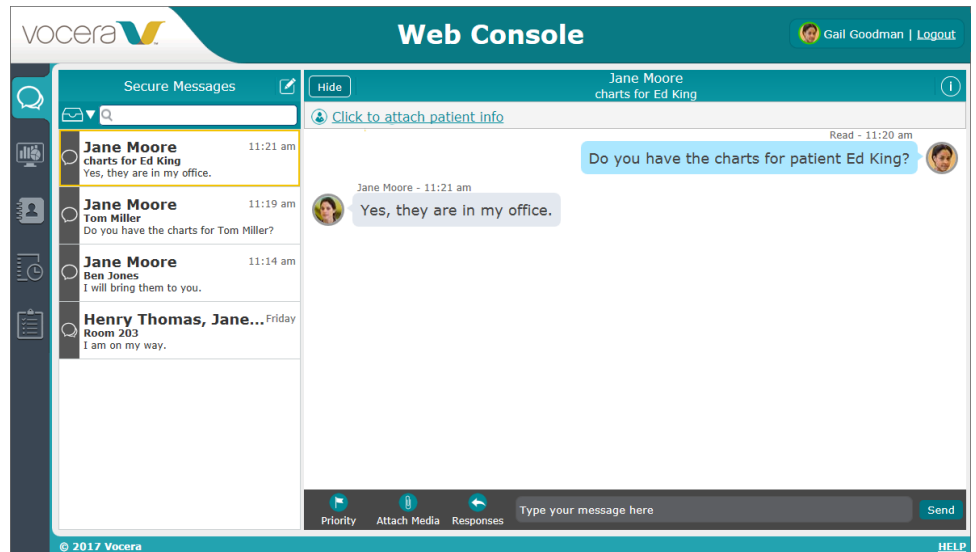
Continuing a Message Conversation

After you have sent or have received a secure message in the VMP Web Console, you can continue a conversation with the recipients or sender of the message.

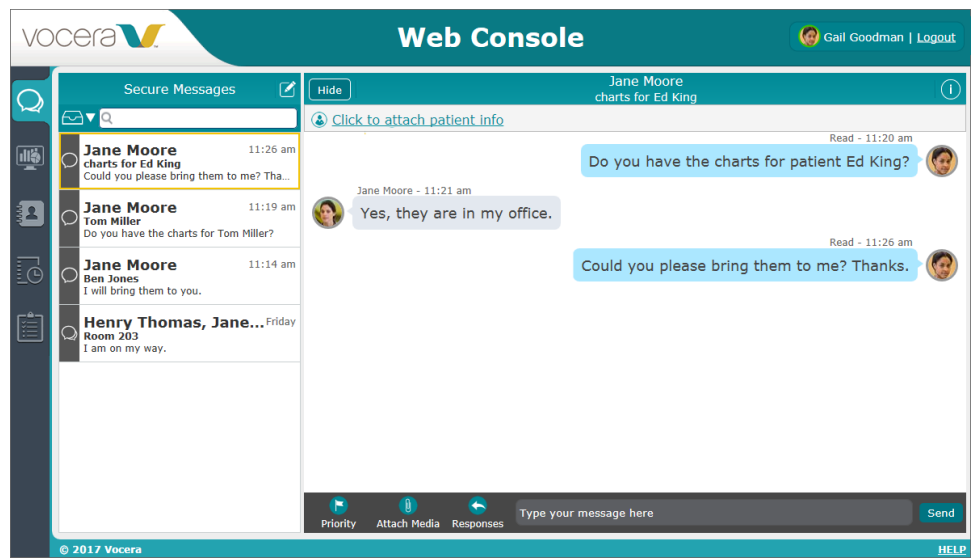
- Select the **Message** tab.



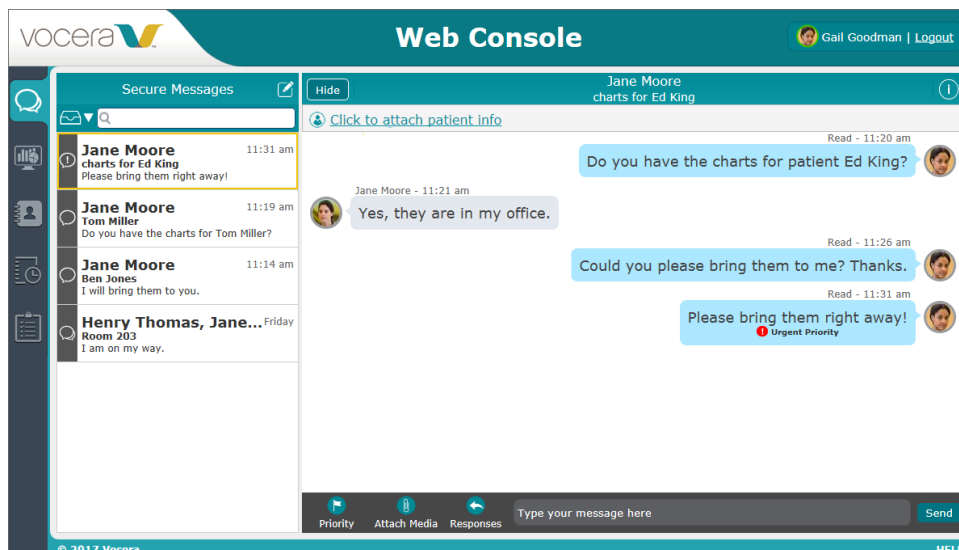
- From the list of messages in the **Secure Messages** pane, select the message. The message is displayed in the pane at the right.



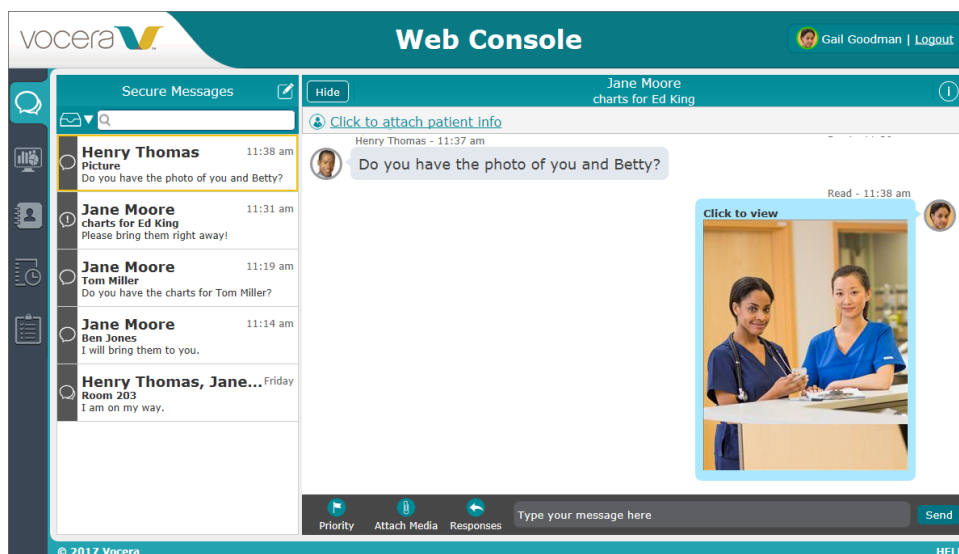
3. In the text field at the bottom of the pane, type your text message and click **Send**. Your messages and the responses sent to you are displayed.



4. To change the priority of a message, click **Priority** and select the priority to use. If the priority is higher than Normal, the priority is included in the message.



5. To attach media to a conversation, click **Attach Media** and select the attachment to include. A thumbnail of the attachment appears in the conversation.



Click the thumbnail to view the attachment in more detail.

6. To request a response to a message, click **Responses**. In the Response Request screen, specify the response information, and click **Send**.

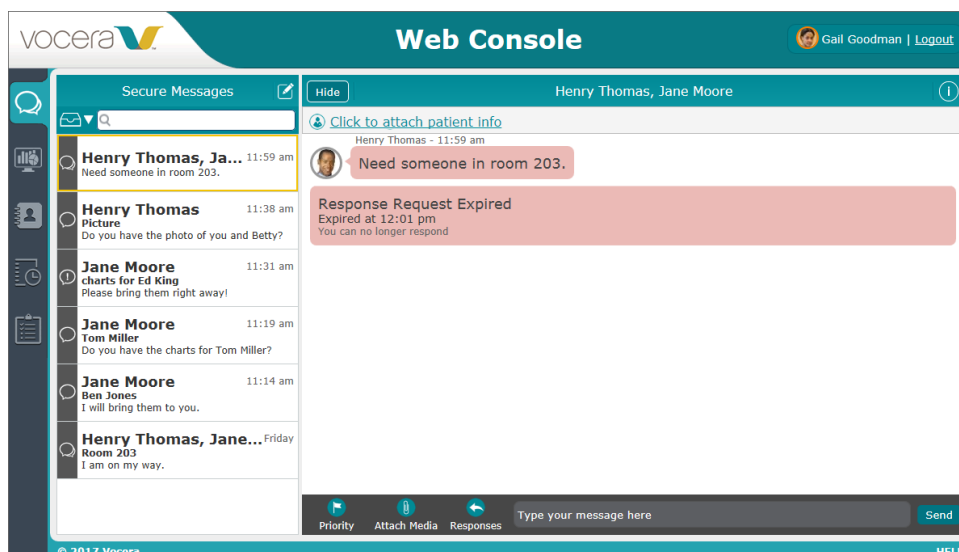
The screenshot shows the Vocera Web Console interface. At the top, the header includes the Vocera logo, the title "Web Console", and a user profile for Gail Goodman with a "Logout" link. The left sidebar contains navigation icons for messages, contacts, and other functions. The main content area is divided into two panes. The left pane, titled "Secure Messages", displays a list of messages from Henry Thomas and Jane Moore. The right pane shows the details of a selected message from Jane Moore to Tom Miller. It includes a "Message:" field, "MESSAGE SETTINGS" (Priority: Normal, High, Urgent; Notify if no one has responded within: minutes), and "RESPONSE OPTIONS" (Response Expiration: Never, 2 min, 5 min, 10 min, Custom). A response field is visible with the text "1: ". At the bottom of the right pane are "Send" and "Cancel" buttons. The footer shows "© 2017 Vocera" and a "HELP" link.

7. If you have been requested to supply a response, a list of response options is provided. Hover over an option to select it, and click the option to send the response.

This screenshot shows the Vocera Web Console interface with a response selection screen. The left pane shows the same message list as the previous screenshot. The right pane now displays a message from Henry Thomas to Jane Moore: "Need someone in room 203." Below the message, a red banner states "Your Response is Required" with the instruction "Tap to select your response". Two response options are listed: "I am on my way." (highlighted in red) and "Sorry, I am busy." Each option has a "Click to Send" button. At the bottom of the right pane are icons for "Priority", "Attach Media", and "Responses", followed by a text input field "Type your message here" and a "Send" button. The footer shows "© 2017 Vocera" and a "HELP" link.



Note: If the sender has specified a time limit for a response, and the time limit has expired, this will be indicated in the conversation:



If you are having more than one conversation, use the pane at the left to switch from one session to another.

To display the current message delivery status, click on any text that you have sent in a conversation.

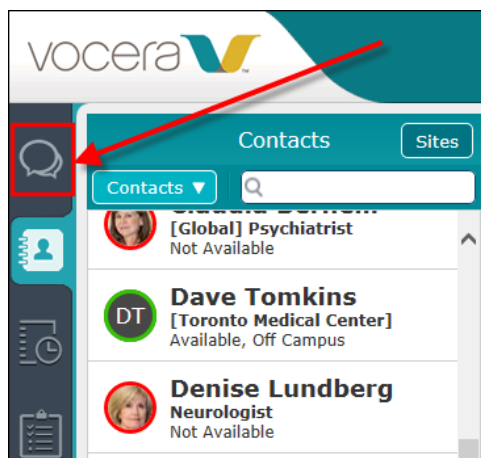
Click on a profile picture to display the contact status information for that person.

If a VST user sends a message, you can see all users who are part of this message, including those VST users who are not part of an organization on the imported VST cloud server and are therefore not in the VMP Server database.

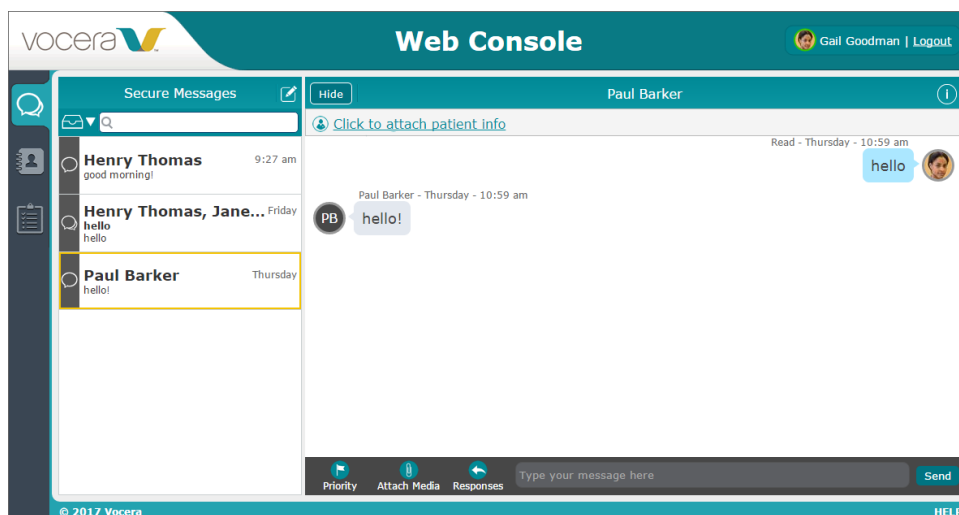
Viewing Participants

You can view a list of the participants in a conversation.

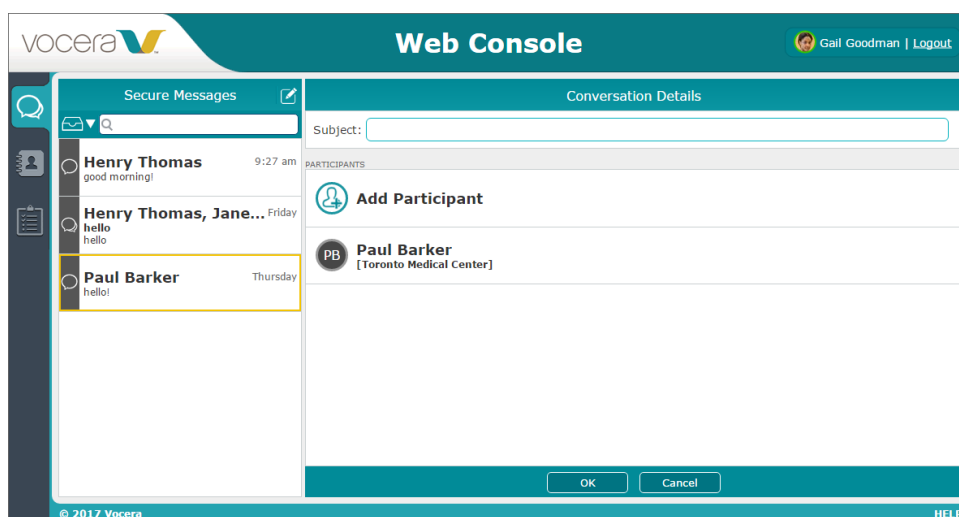
1. Select the Message tab.



2. From the list of messages in the Secure Messages pane, select the message for which you want to view the list of participants.
3. Click the Info icon.



The list of participants appears:

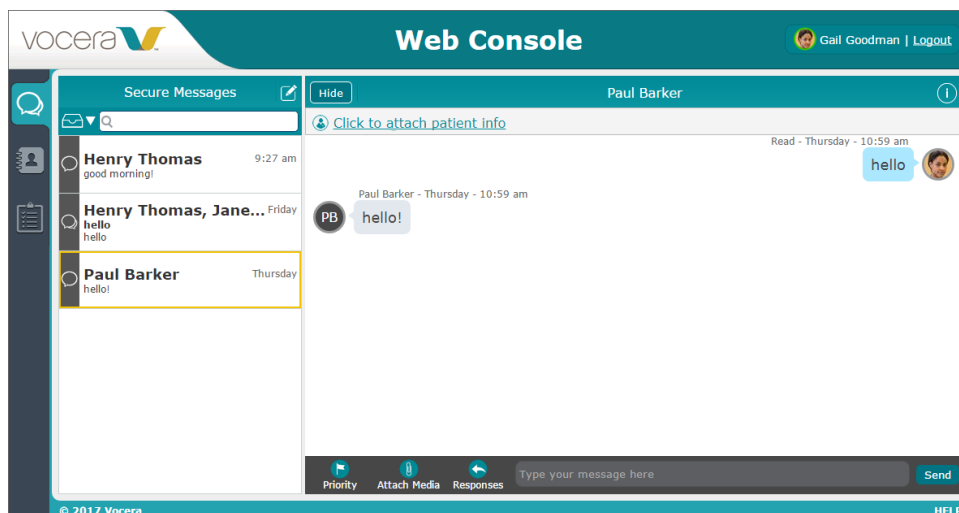


4. Click OK to return to the conversation.

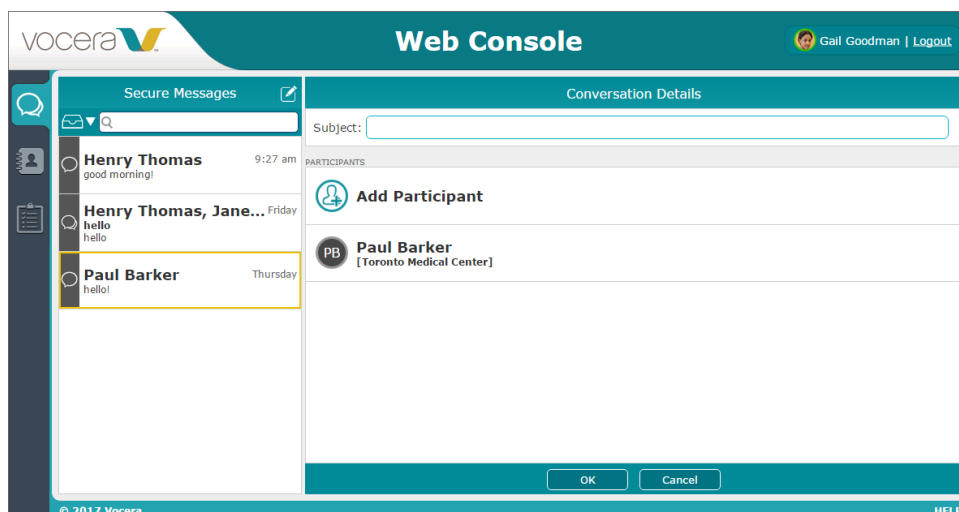
Adding a User to a Message Conversation

You can add additional users to an existing message conversation.

1. Click the Info icon.



The list of participants appears:



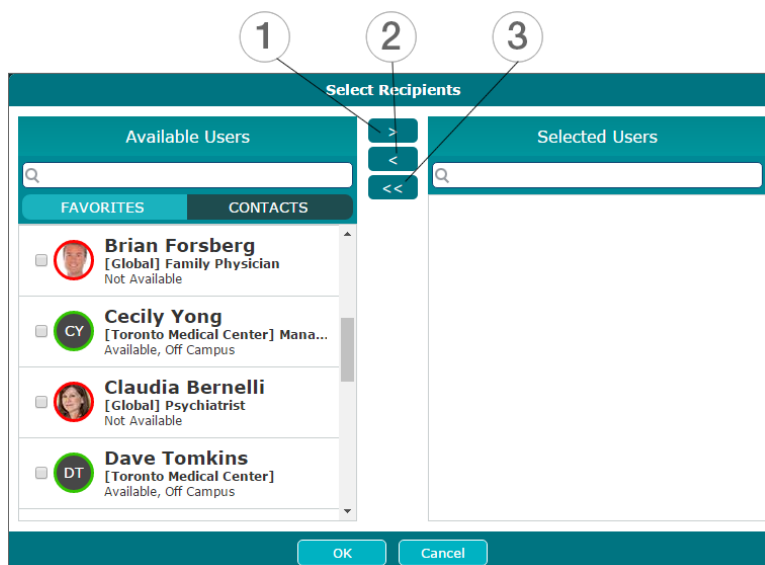
2. Click Add Participant. The Select Recipients dialog box appears.
3. Select the Favorites tab to display favorites only, or select the Contacts tab to display all contacts.



Note: See [Using Web Console Favorites](#) on page 239 for more information on creating favorites.

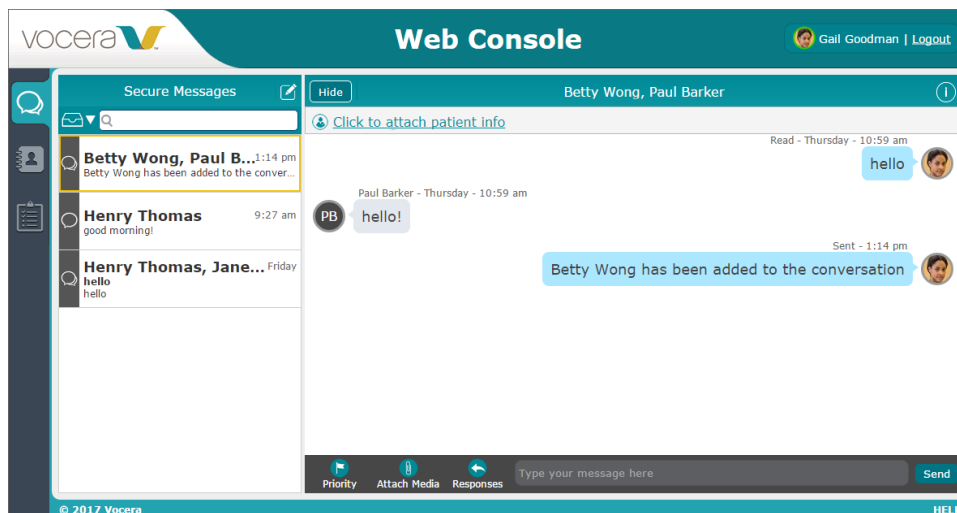
4. Select the checkboxes of the users that you want to add to the conversation:

- 1 Click > to add a user to the conversation.
- 2 Click < to remove a user that you have added to the conversation.
- 3 Click << to remove all users that you have added. You cannot remove users that you have not just added.



5. Click OK to add the selected users to the conversation.

The conversation now indicates that new people have joined.

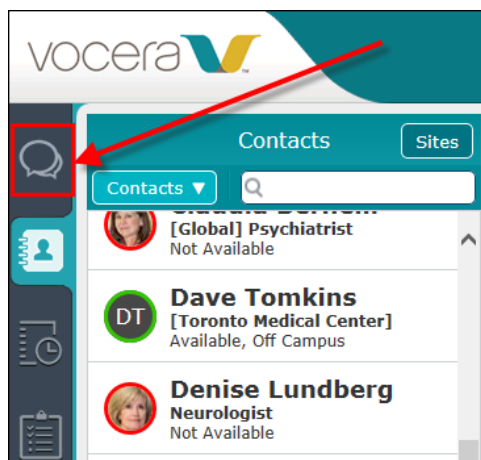


Note: If a user in a message conversation is having messages forwarded to another user, that user is automatically added to the conversation.

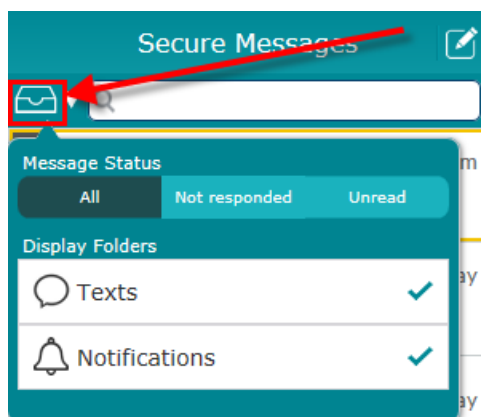
Filtering Message Conversations

You can specify the message conversations that are to be displayed in the Secure Messages screen.

1. Select the Message tab.



2. Click the Inbox icon to display the filtering options.

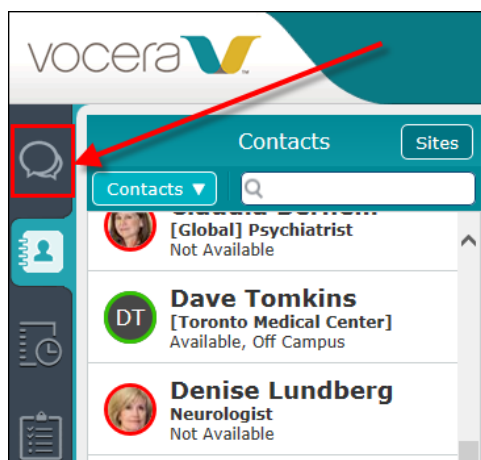


3. In the Message Status section, select whether to display all messages, messages to which you have not responded, or messages that are unread.
4. In the Display Folders section, select **Texts** to display text conversations, and select **Notifications** to display notifications. You can select either or both.
5. Click outside of the filtering options popup menu to hide it. The Secure Messages screen is updated to reflect your selections.

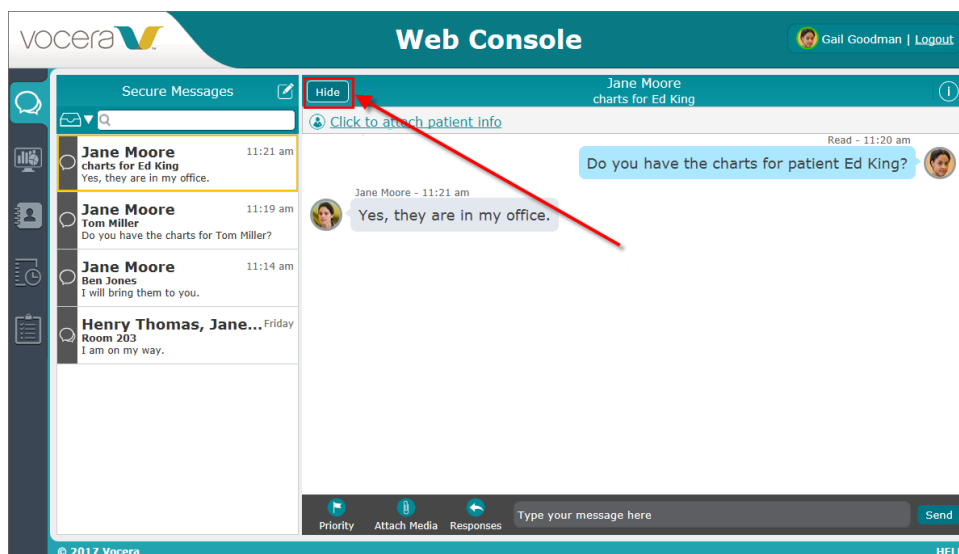
Hiding a Message

If you do not need to save a message, you can hide it.

1. Select the **Message** tab.



2. From the list of messages in the Secure Messages pane, select the message that you want to hide.
3. Click **Hide**.



4. In the Hide Conversation dialog box, click **Yes** to hide the message.



Note: The message reappears if a sender or recipient that has not hidden the message continues the conversation.

Patient Information and Alarms

Your system administrator may have linked your VMP environment to an Engage environment. Two types of Engage environment connections are supported.

- Connections to the Engage Patient Context Adapter, which enable you to add information on a patient to a message conversation.
- Connections from Engage to the VMP SOAP interface, which send alarms sent by patients or care providers to you as notifications.

You can respond to an alarm, view patient information, or contact the care team assigned to the patient.

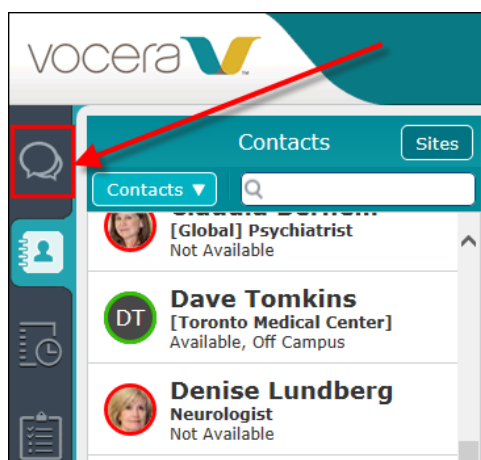


Note: See the Engage product documentation for more details on these adapters.

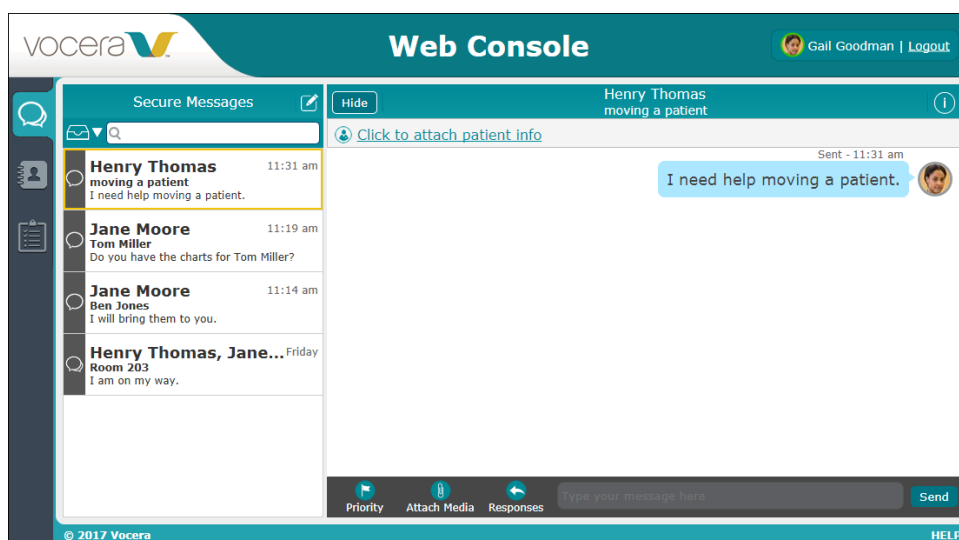
Adding a Patient to a Message Conversation

If patient information is available and no patient has been added to your conversation, you can add patient information if you have permission to do so.

1. Select the Message tab.



2. From the list of messages in the Secure Messages pane, select the message. The message is displayed in the pane at the right.



3. Click the Click to attach patient info link. The Select Patient dialog box appears.

Select Patient

Search by name, room, unit or MRN

MY PATIENTS ALL PATIENTS

Ismael Q. Abel
Room: 7063 DoB: Jan/09/1954
Unit: HATH 07PP
MRN: IsmaelAbel19540109

GABRIEL ACUNA
Room: CC473 DoB: Jun/14/1984
Unit: FACILITY CARDIO
MRN: 12345640202275565

Eugene Y. Adair
Room: 12030 DoB: Mar/14/1973
Unit: HATH 12Med
MRN: EugeneAdair19730314

BARBARA S ADAMS
Room: CC593 DoB: Dec/27/1945
Unit: FACILITY CARDIO
MRN: 1234564020180919

BARBARA S ADAMS
Room: N593 DoB: Dec/27/1945
Unit: FACILITY NICH

OK Cancel

If no patient information is available, this link does not appear.

- Click My Patients to see a list of patients assigned to you, or click All Patients to view a list of all available patients.
- Type text in the search field to limit the patient list to patients whose name matches your search text.
- Select the patient whose information you want to attach to this message.
- Click OK to close the Select Patient dialog box.

The information for the selected patient is now included in the message conversation.

vocera Web Console Gail Goodman | Logout

Secure Messages Hide Henry Thomas moving a patient

BARBARA S ADAMS - Room: CC593 - DoB: Dec/27/1945 (71) View Details

Sent - 11:31 am

Henry Thomas 11:31 am
moving a patient
I need help moving a patient.

Jane Moore 11:19 am
Tom Miller
Do you have the charts for Tom Miller?

Jane Moore 11:14 am
Ben Jones
I will bring them to you.

Henry Thomas, Jane... Friday
Room 203
I am on my way.

I need help moving a patient.

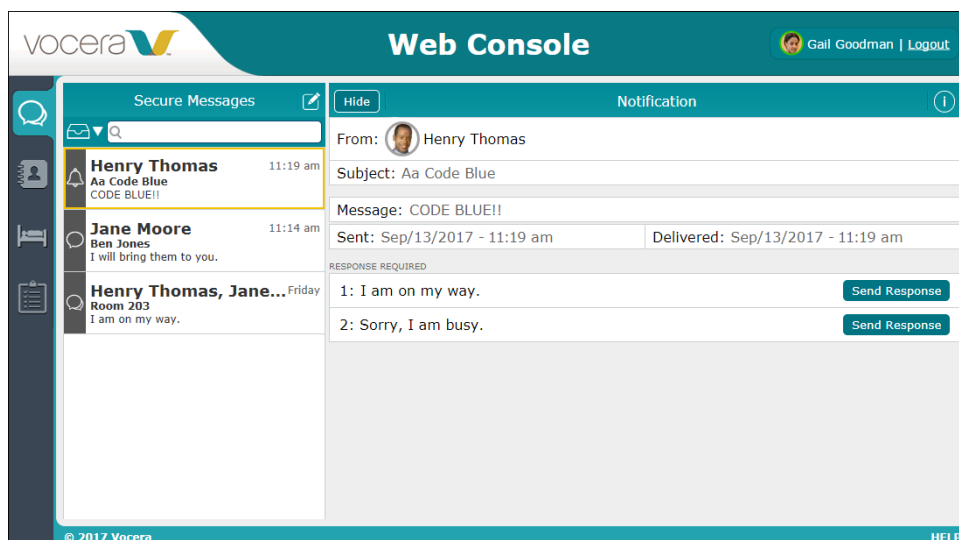
Priority Attach Media Responses Type your message here Send

© 2017 Vocera HELP

Handling an Alarm

If you have received a notification from the VMP SOAP interface that contains information on an alarm generated by or for a patient, you can respond to the alarm, view the information for the patient, and contact the care team assigned to the patient.

- In the Secure Messages screen, click the notification to view it. If necessary, scroll the screen to view the details of the alarm.



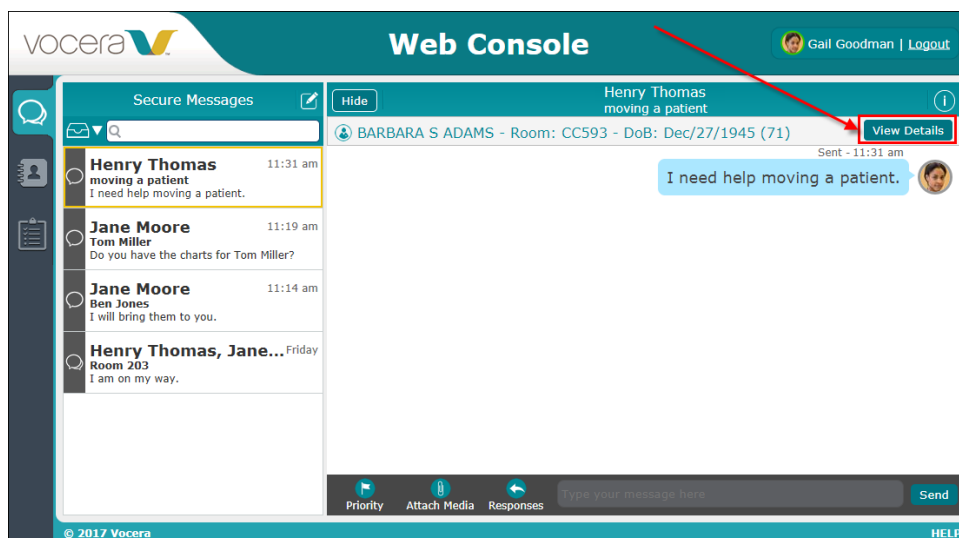
If the alarm has a priority of High or Urgent, an icon appears next to the Subject line.

2. In the Response Required section of the notification, select one of the responses that have been made available to you.
3. Tap the link for the patient to display patient information and contact the care team. See [Viewing Patient Information](#) on page 219 and [Contacting the Care Team](#) on page 220 for more details.

Viewing Patient Information

If you have added patient information to a message conversation, or you have received a notification containing patient information, you can view it.

1. In the Secure Messages screen, click the message or the notification containing the patient information.
2. In the link to the patient information, click the View Details button.



The patient information screen appears.

Vocera Web Console

Secure Messages

Henry Thomas moving a patient 8:56 am
I need help moving a patient.

Jane Moore Room CC593 Yesterday
You are needed in room CC593

Jane Moore Code Blue Yesterday
There is a Code Blue in ER

Patient Info

BARBARA S ADAMS - Room: CC593 - DoB: Dec/27/1945 (71)

MRN No: 1234564020180919
Gender: Female
Admit Date: 2012-12-08T21:10:00.000-05:00
Discharge Date:
Admit Reason:
Patient Status: Admitted

Care Team

Ace Cline

Henry Thomas [Global] Family Physician Not Available

Jane Moore [Global] Dermatologist Not Available, Messages Forwardi...

John Smith [Global] Oncologist Not Available

Martin Choi [Global] Family Physician Not Available

Text Care Team

© 2017 Vocera

This screen contains two panes:

- The Patient Info pane, which contains details on the linked patient.
- The Care Team pane, which contains links to contact information for care team members.

3. Click **Close** to hide the patient information.

Contacting the Care Team

If you have added patient information to a message conversation, or you have received a notification containing patient information, you can view and contact the care team assigned to this patient.

1. In the Secure Messages screen, click the message or the notification containing the patient information.
2. In the link to the patient information, click the **View Details** button.

Vocera Web Console

Secure Messages

Henry Thomas moving a patient 11:31 am
I need help moving a patient.

Jane Moore Tom Miller 11:19 am
Do you have the charts for Tom Miller?

Jane Moore Ben Jones 11:14 am
I will bring them to you.

Henry Thomas, Jane... Room 203 Friday
I am on my way.

Patient Info

BARBARA S ADAMS - Room: CC593 - DoB: Dec/27/1945 (71)

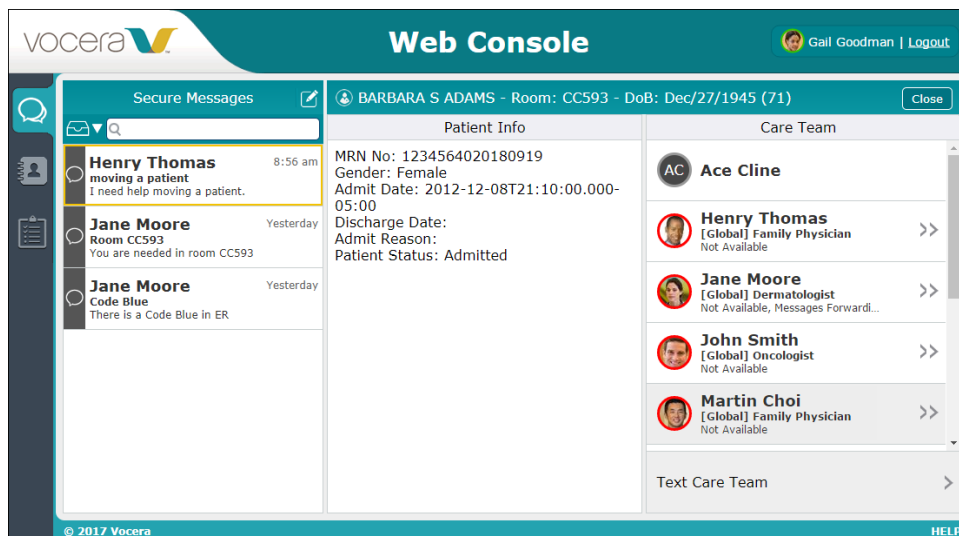
View Details

I need help moving a patient.

Priority Attach Media Responses Type your message here Send

© 2017 Vocera

The patient information screen appears, including the Care Team pane, which displays a list of care team members in a scrollable window.



This list of care team members can contain users from either or both of two sources:

- VMP Web Console or VCS users
- Users obtained from the Engage Patient Context Adapter

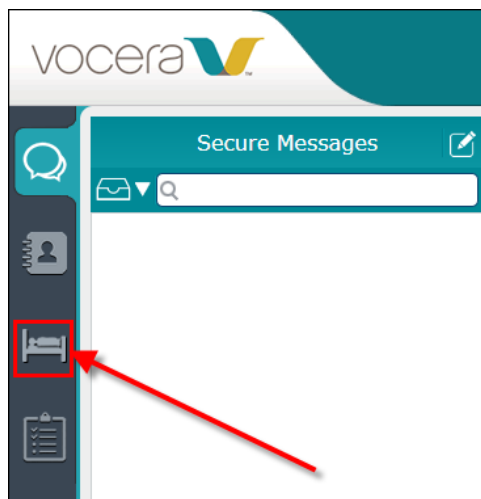
Users obtained from the Engage Patient Context Adapter cannot be contacted from VMP Web Console.

3. In the list of care team members, click on any VMP Web Console or VCS user to display contact information for that user. See [Using Web Console Contacts](#) on page 236 for more details on this contact information.
4. To send a message to all care team members who are VMP Web Console or VCS users, click the Text Care Team link at the bottom of the screen.
The Text Care Team link does not appear if the care team does not include any VMP Web Console or VCS users.
5. Click Close to hide the patient information.

The Patients View

If you have linked your VMP Server to an Engage environment, the Patients view lists all current patients.

1. To access the list of current patients, select the Patients view.



The list of patients appears.



Note: If there are more than 100 patients in the list, not all patients are displayed. Use the search box to search for any patient in the list, including those that are not displayed.

2. Select the patient for which you want to display information.

The patient information consists of two panes:

- The Patient Info pane, which contains details on the linked patient.
- The Care Team pane, which contains links to contact information for care team members.

3. In the list of care team members, click on any VMP or VCS user to display contact information for that user. See [Using Web Console Contacts](#) on page 236 for more details on this contact information.
4. To send a message to all care team members who are VMP or VCS users, click the Text Care Team link at the bottom of the screen.

The Text Care Team link does not appear if the care team does not include any VMP or VCS users.

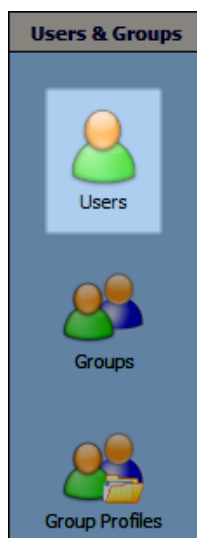
About User Permissions

As an administrator, you can provide user permissions for access to the VMP Web Console, for creating and managing schedules, and for Messages sent by other users.

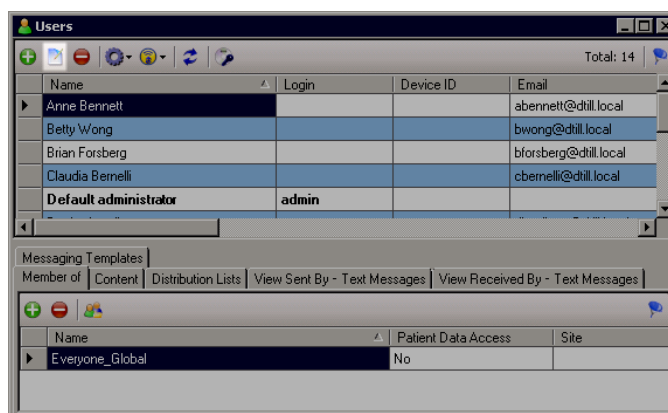
Granting Existing Users Access to the VMP Web Console

You can grant access to any user at any time by editing the user or contact record.

1. Start the VMP Administrator:
All Programs > VMP Administrator
2. Select Users & Groups > Users.



3. Click to highlight the desired user, and click the Edit icon.



The End-User Settings window appears.

4. Click to select Enable Web Console Access.

Edit User

Step 1: End-User Settings

Step 1: End-User Settings
Step 2: Push Technology and Licensing

First Name: John
Middle Name:
Last Name: Smith
Title:
Email: jsmith@dhill.local
Public ID:
Pager ID:
Vocera ID: u-jsmith
Home Site: Global
VST ID:

Auto Forwarding
Allow Forwarding: Follow System Settings (Yes)
Forward To: Remove

Desktop and Web Access
☐ Enable PC Admin Console Access
☒ Enable Web Console Access

Vocera credentials
Login:
Password:
Confirmation:

Next > Cancel Help

5. Provide the authentication credentials, and click Next.
6. Click Next and click Finish to save the edited account and complete the task.

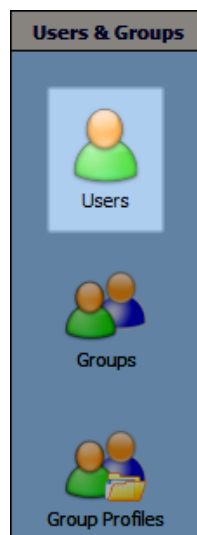


Note: You can grant VMP Web Console access to multiple users at once when importing users and contacts. See [Synchronizing Users and Contacts](#) on page 60 for more details.

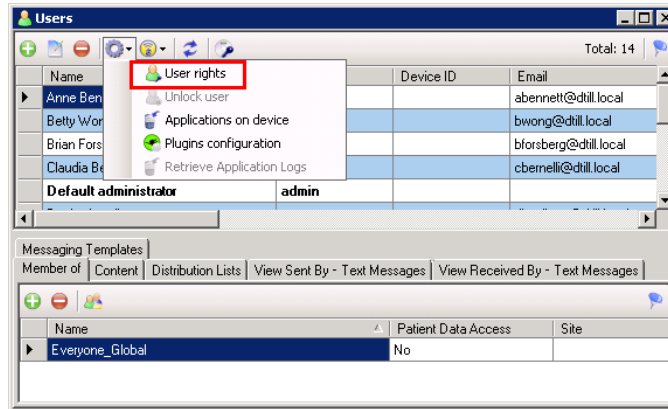
Granting Users Scheduling Permissions

You can grant permissions to enable a user to create and manage schedules in the VMP Web Console.

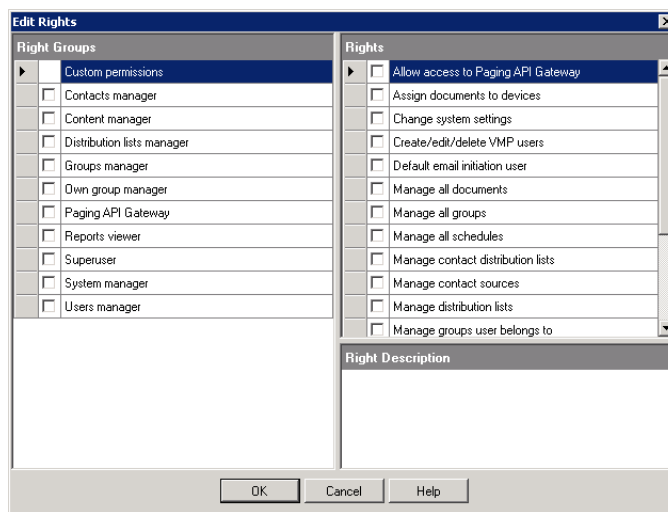
1. Start the VMP Administrator:
All Programs > VMP Administrator
2. Select Users & Groups > Users.



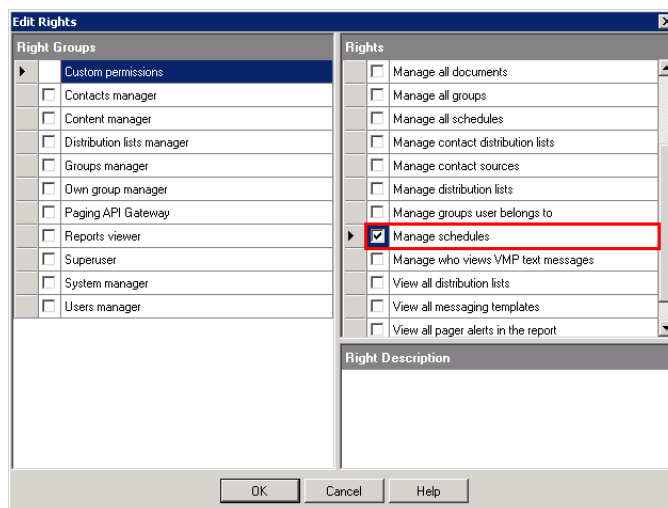
3. In the Users pane, click the name of the user for which user rights are to be edited.
4. In the toolbar, from the User preferences dropdown list, select User rights.



The Edit Rights dialog box appears.



5. In the Right Groups pane, select Custom permissions.
6. In the Edit Rights dialog box, select the Manage schedules checkbox. This user right allows the user to create schedules and to edit the schedules that he or she has created.



Note: If Manage schedules has already been selected and cannot be changed, this user has already been granted the right to manage schedules as part of a Right Group. See [Editing User Rights](#) on page 123 for more details.

7. In the Edit Rights dialog box, select the Manage all schedules checkbox to allow this user to edit all schedules that anyone has created.
8. Click OK to finish editing user rights.

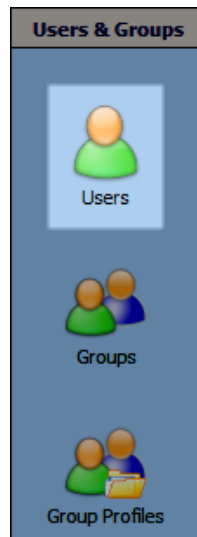


Note: The default administrator always has permission to access schedules. At least one user must be given permission to manage schedules.

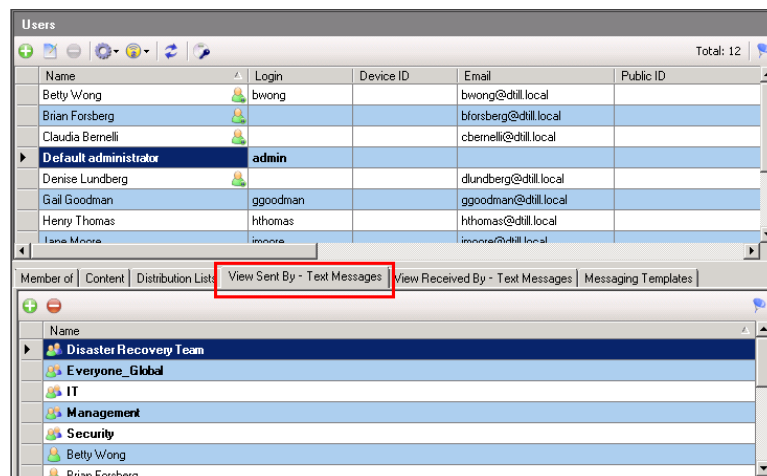
Allowing Users to View Messages

You can give one or more users the ability to view messages sent by or received by other users. This enables access to the Monitor View in the VMP Web Console.

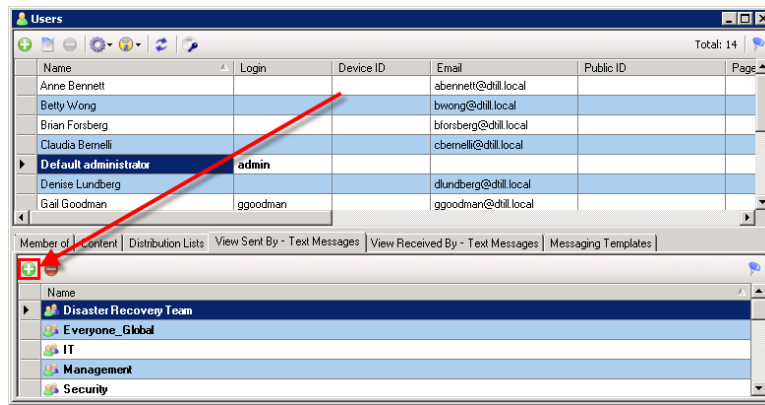
1. Start the VMP Administrator:
All Programs > VMP Administrator
2. Select Users & Groups > Users.



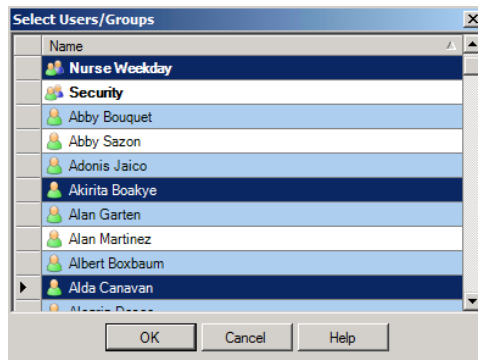
3. Highlight the users to which you want to grant permission to view sent messages, and click the View Sent By - Text Messages tab at the bottom of the user list.



4. Click Add.



5. Highlight the users and groups whose sent messages can be viewed, and click OK.



6. Highlight the users to which you want to grant permission to view received messages, and click the **View Received By - Text Messages** tab at the bottom of the user list.
7. Click **Add**.
8. Highlight the users and groups whose received messages can be viewed, and click **OK**.

On-Call Status and Schedules

You can use the VMP Web Console to specify on-call status and create schedules.

If On-Call Scheduling has been provided with the VMP Server, you can use the **On-Call** view to update your own on-call status or the on-call status of other users.

You can also use the **Schedules** view to create schedules based on On-Call Distribution Lists (DLs). See [Creating a Regular or On-Call Distribution List](#) on page 152 for more information about creating On-Call DLs.

Schedules can be copied from existing schedules, can be drafted and remain unpublished, and can be published at any time.

You can view schedules by:

- Day
- Week
- Month
- Shifts

For information on how to grant users the right to change their own status, see [Creating a Regular or On-Call Distribution List](#) on page 152.

For information on how to grant users the permission to manage schedules, see [Granting Users Scheduling Permissions](#) on page 224.

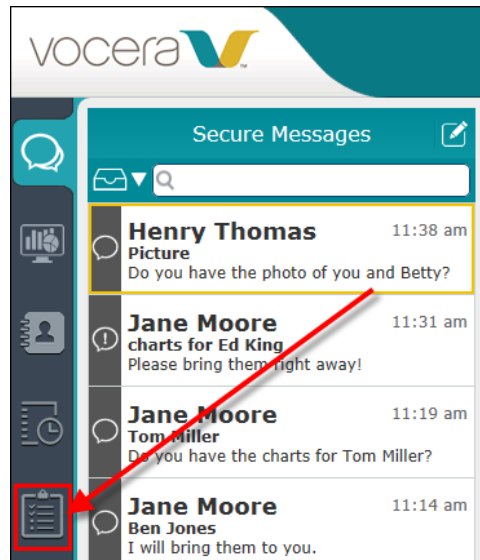


Note: To determine whether On-Call Scheduling has been provided, start the VMP Enterprise Manager, select Instances, and click your license key. In the Modules pane, check the value of the On-Call Scheduling field.

Modifying Your On-Call Status

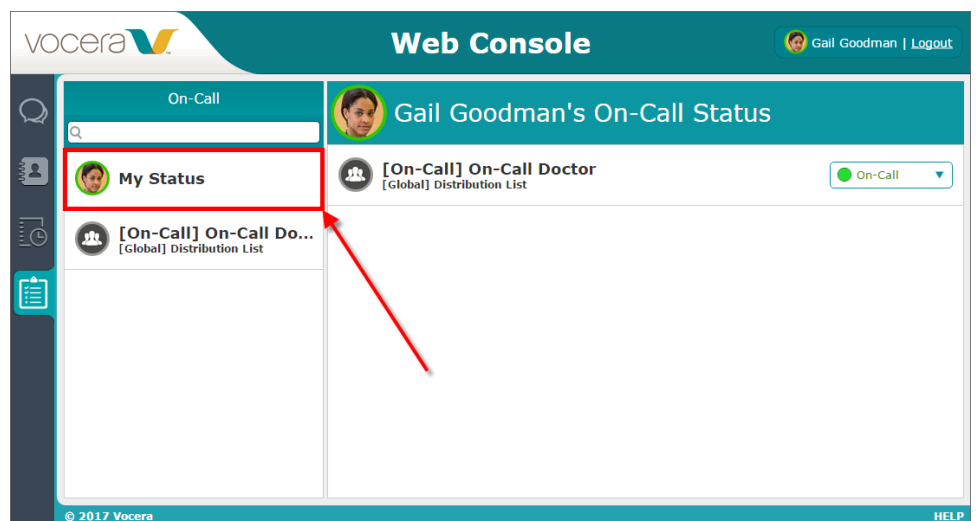
You can change your on-call status in any schedule that includes you.

1. Open the VMP Web Console from your Web browser.
2. Click On-Call.

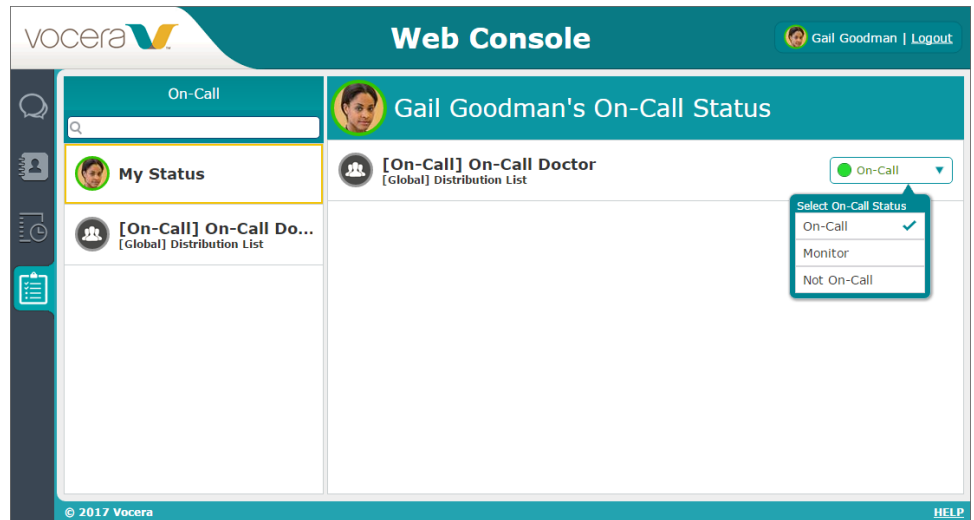


This icon appears only if you have access to On-Call Distribution Lists.

3. In the On-Call Lists pane, click My Status. A list of the Distribution Lists to which you belong is displayed, along with your on-call status for each.



4. For the Distribution List for which you want to change your on-call status, click your current status. A list of options appears.



5. Change your status to one of the following:

- On-Call - Receive messages sent to the list.
- Monitor - Receive message sent to the list, but a response is not expected even when a message requires one.
- Not On-Call - Do not receive messages sent to the list.

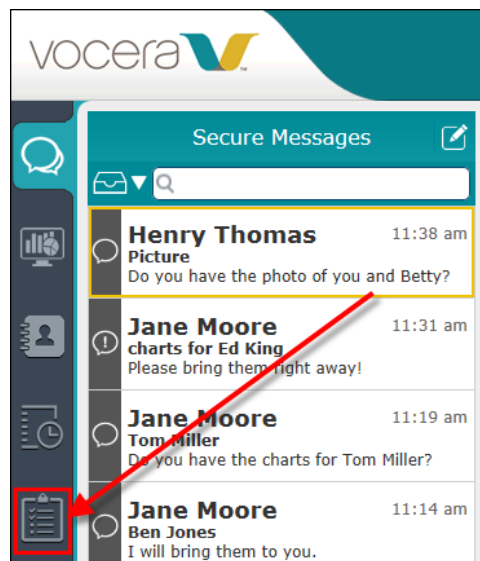


Tip: Select Monitor to receive messages sent to the list without the expectation of a response or action for the message. A shift manager might find it useful to monitor the shift and ensure that messages are handled appropriately.

Modifying Any On-Call Status

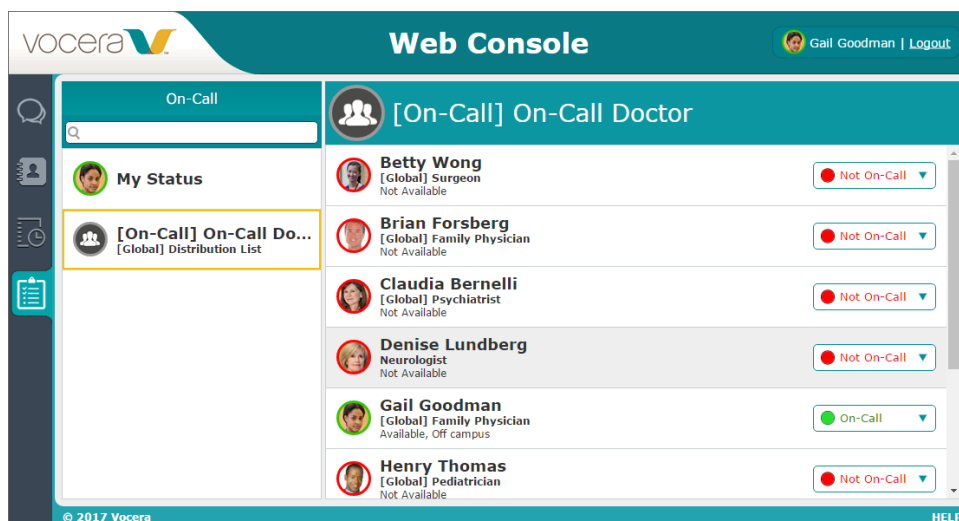
You can modify the on-call status of any user in a Distribution List.

1. Open the VMP Web Console from your Web browser.
2. Click On-Call.

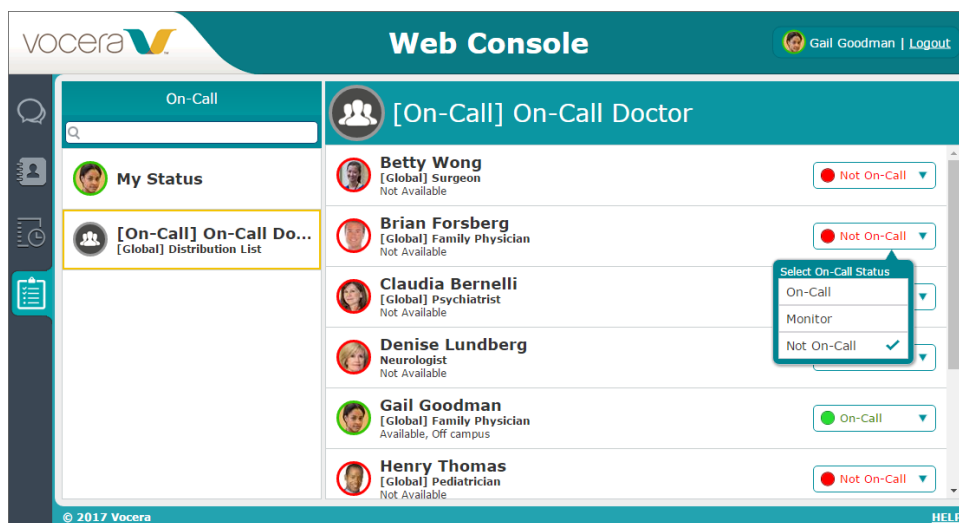


This icon appears only if you have access to On-Call Distribution Lists.

3. In the On-Call Lists pane, click the Distribution List that you want to update. A list of users is displayed, along with their on-call status.



4. For the user whose on-call status you want to change, click the user's current status. A list of options appears.



5. Change the user's status to one of the following:
- On-Call - Receive messages sent to the list.
 - Monitor - Receive messages sent to the list, but a response is not expected even when a message requires one.
 - Not On-Call - Do not receive messages sent to the list.



Note: At least one user in the Distribution List must have a status of On-Call at all times.

If you do not want to update a user's on-call status, tap the list name at the top left of the screen to return to the list of users.

6. Repeat the above step until all users have had their on-call status changed as needed.

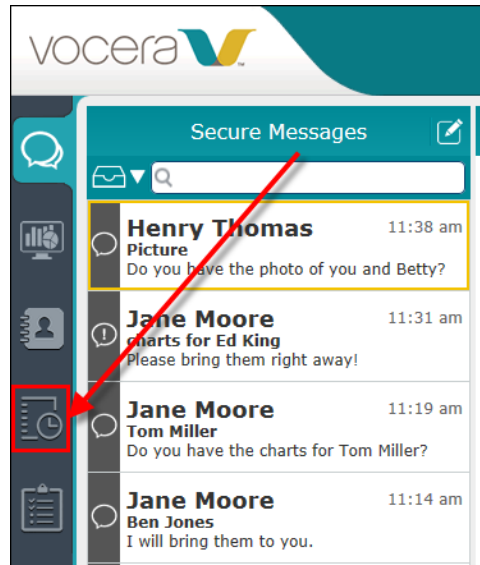
Creating On-Call Schedules

A logged in user can use the VMP Web Console to create an on-call schedule if you have used the VMP Administrator to grant permission to do so.



Note: For details on granting scheduling permissions, see [Granting Users Scheduling Permissions](#) on page 224.

1. Open the VMP Web Console in your Web browser.
2. Click Schedule.



The list of schedules appears.



3. Click New Schedule.



Note: If you do not have permission to create on-call schedules, the New Schedule button is not available.

4. Enter a meaningful Schedule Name.

New Schedule

Schedule Name:

Schedule Distribution List:

[On-Call] Walk-In Clinic Doctors

▼

Schedule Start Date:

Time Zone:

(UTC-05:00) Eastern Time (US & Canada)

▼

☒ Daylight saving

Minimum # of On-Call Users per Shift:

☒ Enable Automatic Validation

5. Use the Schedule Distribution List dropdown list to select the On-Call Distribution List (DL) for the schedule.
6. Click in the Schedule Start Date field to open the calendar picker and select the start date.

May 2015						
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

7. If needed, use the Time Zone dropdown list to select the appropriate time zone, or select the Daylight saving checkbox.
8. In the Minimum # of On-Call Users per Shift field, enter the minimum number of users that are to be specified as on-call in each shift.
9. Select the Enable Automatic Validation checkbox if the VMP Server is to perform automatic validation of this schedule to ensure that all shifts have enough on-call users.
10. If you want to copy the shifts for the new schedule from an existing schedule, click to activate the Copy shifts from an existing Schedule checkbox, and select the schedule from the dropdown list.

☒ Copy shifts from an existing Schedule

Copy shifts from: On-Call Doctors

11. Use the Permissions pane to select Users/Groups with permission to view or manage the schedule. Click to activate the checkbox next to the desired user or group and click > to select.

Available Users/Groups			Selected Users/Groups		
<input type="text"/>		>> > < <<	<input type="text"/>		
Name			Name View Manage		
<input type="checkbox"/> BW Betty Wong			<input type="checkbox"/> D Default administrator		
<input type="checkbox"/> BF Brian Forsberg			<input checked="" type="checkbox"/>		
<input type="checkbox"/> CB Claudia Bernelli				<input checked="" type="checkbox"/>	

12. Click OK to continue.
13. Click the name of the schedule to continue editing it.
14. Use the arrow buttons or the calendar picker to select a date for which to schedule shifts.

15. To assign a shift to a user, drag the user's name to the time slot that is to be the start of the shift. Use the Shift Period dialog to specify the start time and the end date and time for the shift.

Shift Period

Start Time: Dec 21 11 am 00
End Time: Dec 21 12 pm 00

OK
Cancel



Tip: To change the times for a user's shift, drag the shift assignment to the desired time slot. Drag the bottom of the shift assignment to increase the number of assigned hours.

16. Repeat the above step to add users to the schedule as appropriate. You can schedule more than one user in any time slot.
17. When you have finished creating the shift assignments, click Repeat to copy these assignments to other days of the month:

Repeat Day

Repeat
☐ Every Sunday
☒ Every Monday
☒ Every Tuesday
☒ Every Wednesday
☒ Every Thursday
☒ Every Friday
☐ Every Saturday
Repeat from to

OK
Cancel

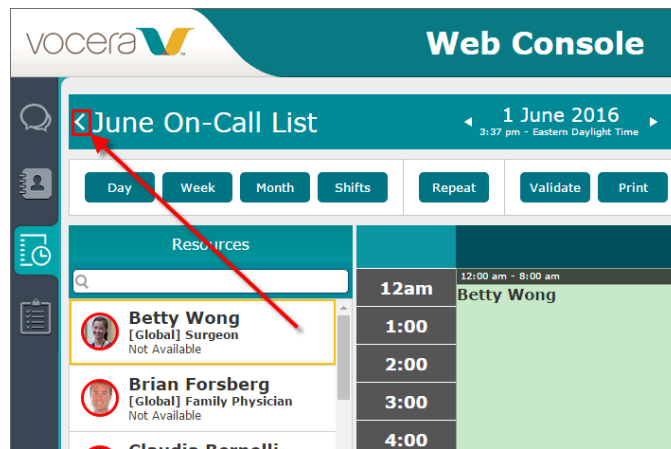
- a. Use the checkboxes to specify the days of the week on which these shifts are to be assigned.
 - b. Click in the Repeat from field to specify the start of the date range in which these shifts are to be assigned.
 - c. Click in the to field to specify the end of the date range.
 - d. Click OK.
18. Click Week or Month to view the shift assignments for a specific week or month. To view the shift assignments for a specific user, click Shifts and then click the user's name.
- In the Week or Month view, you can copy shift assignments from one day to another:

- a. Locate the day of the month whose shift assignments you want to copy. Click on the heading for that day of the month to highlight it.

	Sun, 24	Mon, 25	Tue, 26	Wed, 27	Thu, 28
12am	12:00 am X Betty W...	12:00 am X Betty W...	12:00 am X Betty W...	12:00 am X Betty W...	12:00 am X Betty W...
1:00					
2:00					
3:00					

- b. Click Copy.
 - c. Locate the day of the month to which you want to copy the shift assignments. click the heading for that day of the month to highlight it.
 - d. Click Paste. The shift assignments are copied to the specified day.
19. To ensure that all shifts have enough on-call users, click Validate. This checks all days for which shifts are scheduled, up to the (possibly partial) last day. A pop-up dialog appears that either lists the shifts for which not enough on-call users are defined or indicates that the schedule is valid.

20. When the schedule is complete, click the back arrow to return to the Schedule list.

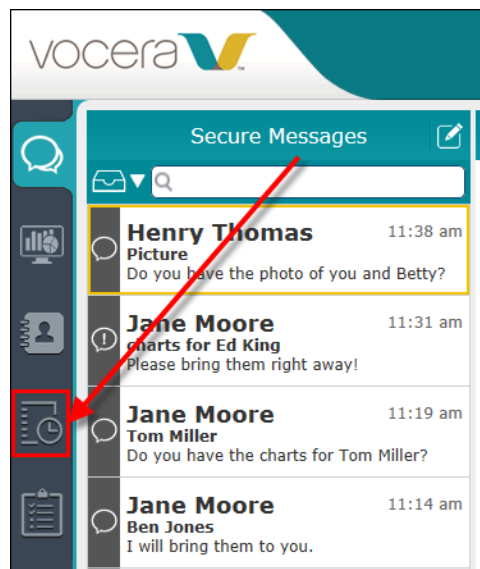


21. Select the Published checkbox to publish the schedule.

Viewing the Schedule Dashboard

From the VMP Web Console, you can view the Schedule Dashboard, which lists any or all the schedules that you have created and who has been assigned shifts in these schedules for any specific day.

1. Open the VMP Web Console in your Web browser.
2. Click Schedule.



3. Click Dashboard.
4. Click Select Schedules.
5. To select a schedule, go to the *Available Schedules* pane, select the checkbox next to the schedule, and click >. To unselect a schedule, go to the *Selected Schedules* pane, clear the checkbox next to the schedule, and click <.

Select DL's/Users

Search:

☐ **On-Call Doctors**

☐ **Walk-In Clinic Doctors**

Navigation: >>, >, <, <<

Drag and drop to sort

OK Cancel

You can select a maximum of 20 schedules.

6. To change the order in which the schedules are to be displayed, drag and drop the schedules in the **Selected Schedules** pane as needed.
7. Click **OK**. The **Schedule Dashboard** now displays the schedules that you have selected. For each schedule, the shifts assigned for the current date are displayed.

Schedules Dashboard		26 May
Select Schedules	On-Call Doctors	Walk-In Clinic Doctors
12am	12:00 am - 3:00 pm Betty Wong	12:00 am - 6:00 am Brian Forsberg
1:00		
2:00		
3:00		
4:00		
5:00		
6:00		6:00 am - 3:00 pm Claudia Bernelli
7:00		
8:00		
9:00		
10:00		

8. To view the shifts for a different date, select the date from the calendar at the top right of the **Schedule Dashboard**, or use the arrow icons to navigate to the date that you want to display.

Schedules Dashboard		26 May
Select Schedules	On-Call Doctors	Walk-In Clinic Doctors
12am	12:00 am - 3:00 pm Betty Wong	12:00 am - 6:00 am Brian Forsberg

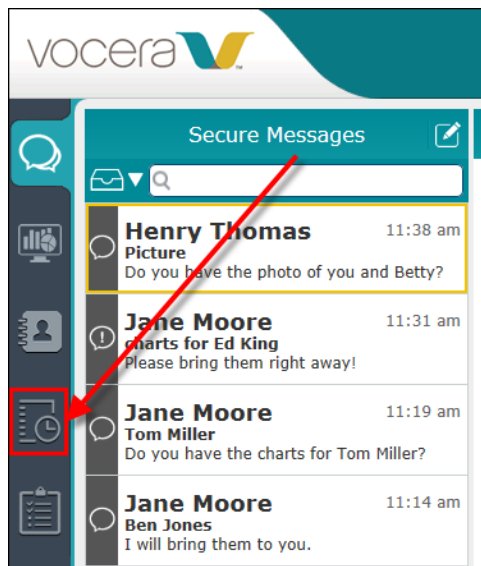
9. Click the **Back** icon to return to the list of schedules.

Schedules Dashboard		26 May
Select Schedules	On-Call Doctors	Walk-In Clinic Doctors
12am	12:00 am - 3:00 pm Betty Wong	12:00 am - 6:00 am Brian Forsberg

Printing a Schedule

You can print a schedule that you are editing. The portion of the schedule that is printed is identical to the portion that you are viewing. For example, if you are viewing the schedule for the current week, the printed schedule is for that week.

1. Open the VMP Web Console in your Web browser.
2. Click Schedule.



3. Click the name of the schedule to display.
4. Click one of Day, Week, or Month to display the schedule for that time period.
5. Click Print. A print window appears that displays the schedule to be printed.
6. In the print window, click Print. This displays the Windows print command window. From this window, select the desired printer and options.

Web Console Contacts

The Web Console Contacts view shows all contacts the logged in user is allowed to access.



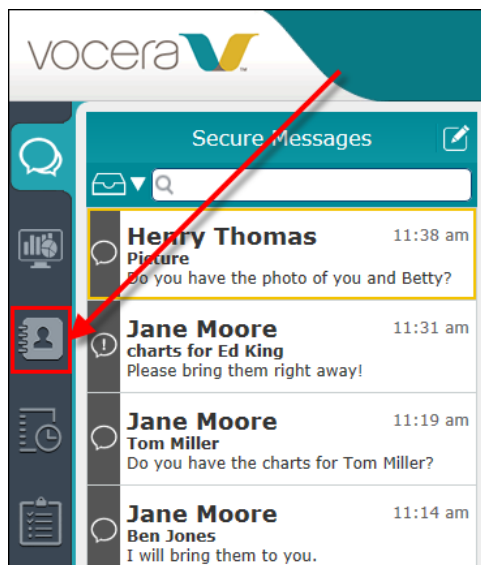
Note: Contact access is defined in the VMP Administrator. For details about defining contacts distribution lists, see [Contacts](#) on page 138.

Using Web Console Contacts

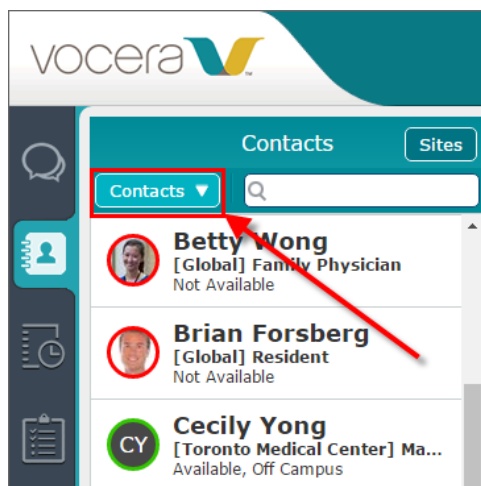
Use the Contacts view to initiate a communication with a contact.

The Email option is available only for users, and is available only if the VMP Server administrator has allowed email communication. Only messages can be sent to group contacts.

1. Log on to the VMP Web Console from your Web browser.
2. Click [Contacts](#) to display the Contacts view.

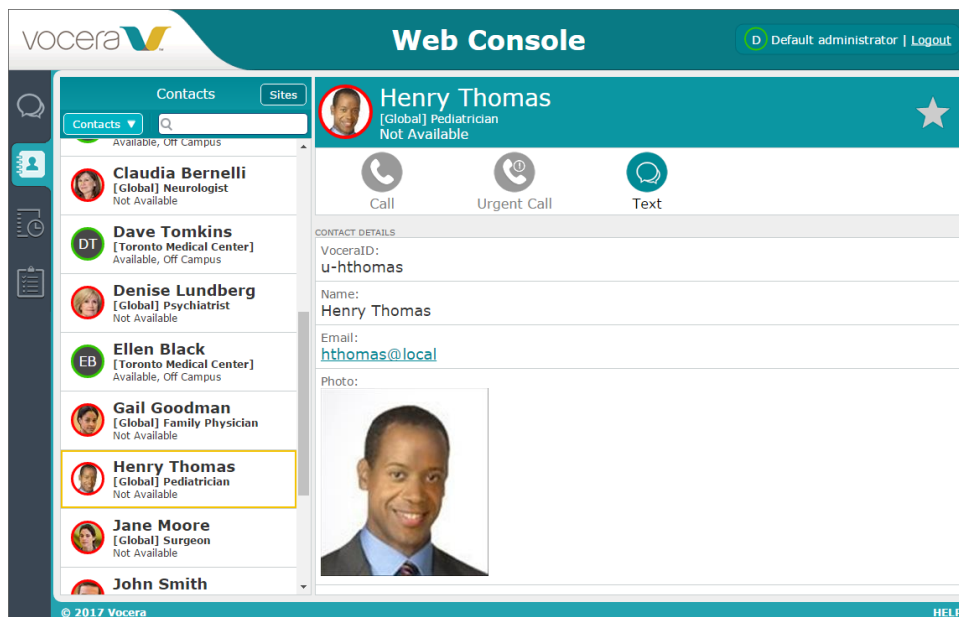


3. Toggle between Favorites or Contacts at the top of the Contacts pane.

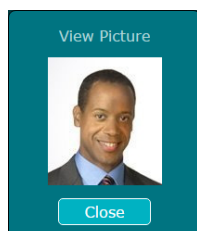


Tip: Start typing the contact name in the search box to quickly find a user, group, or Distribution List. For details on using Favorites, see [Using Web Console Favorites](#) on page 239.

Select a contact to display it:



4. If the contact has a photo, click on it to display it in a separate window:



Click Close to close this window.

5. If a contact is a Vocera Voice Group, the group may contain subgroups. Click the subgroup you want to view. When viewing a subgroup, click the Back arrow to return to the parent Voice Group.
6. When you have found the contact, select Call, Urgent Call, or Text to communicate with the contact. If the contact is a Voice Group or Distribution List, you can send a Broadcast or Urgent Broadcast to all members of the group or Distribution List.



Note: The Call, Urgent Call, Broadcast, and Urgent Broadcast operations are initiated on your client application (VCS client or Vocera badge).

Contact Types and Status

Vocera categorizes contacts as individual users, Voice Groups, and Distribution Lists.

For each user, a colored ring around the user's photo or initials indicates the user's presence and availability:

- Green indicates that the user is available.
- Yellow indicates that the user is in Do Not Disturb mode for calls, messages, or both.
- Red indicates that the user is not available.

For all contacts, the site that the contact belongs to is enclosed in square brackets:

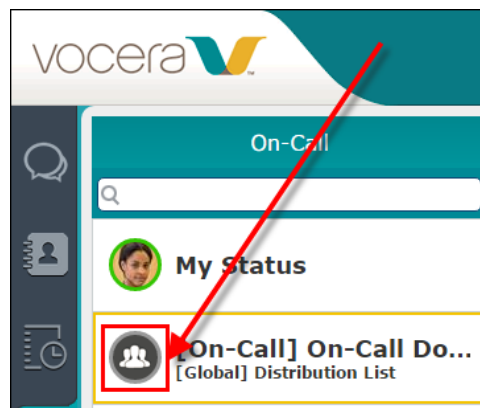
- If Vocera Secure Texting users are included in the list of contacts, the site for each Vocera Secure Texting user is the organization to which that user belongs.
- If you have not created any sites, all contacts other than Vocera Secure Texting users have the site name [Global].

For each user, details on the user's current status are provided below the contact's name, site, and title. These include the following:

- The contact's availability status, corresponding to the colored ring around the user's photo or initials. This is one of *Available*, *Do Not Disturb*, or *Not Available*. For *Do Not Disturb*, the current status indicates whether calls, messages, or both or are not being let through.
- *Messages Forwarding* indicates that messages to this contact are being forwarded to another contact.
- *Off Campus* indicates that the contact is available but is not on the corporate network. An example of this is when the contact is logged into the VMP Web Console.

Vocera Secure Texting users are listed as *Available* and *Off Campus*.

Voice Groups and Distribution Lists are indicated with a multi-person icon.

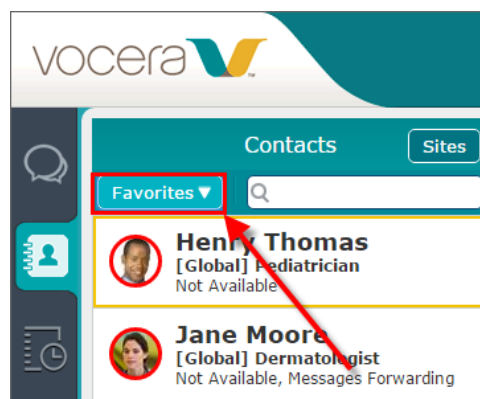


For each user in a Voice Group or a Distribution List, a photo of the user and the availability status are displayed. If the user has no photo, the user's initials are displayed.

Using Web Console Favorites

In the VMP Web Console, you can specify a list of Favorite contacts that you communicate with frequently.

To display the list of Favorites, select *Favorites* at the top of the Contacts pane.



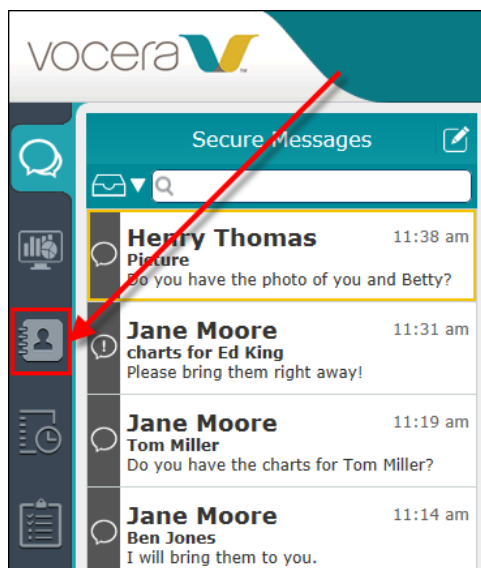
Adding a Favorite

You can add a contact to the list of Favorites.



Note: If a Favorite is a Vocera user, the contact status for the user is displayed in the Favorites list. This lets you quickly determine if the Favorite is logged in to the Vocera system. See [Contact Types and Status](#) on page 238 for more information on contact status.

1. Click Contacts to display the Contacts view.

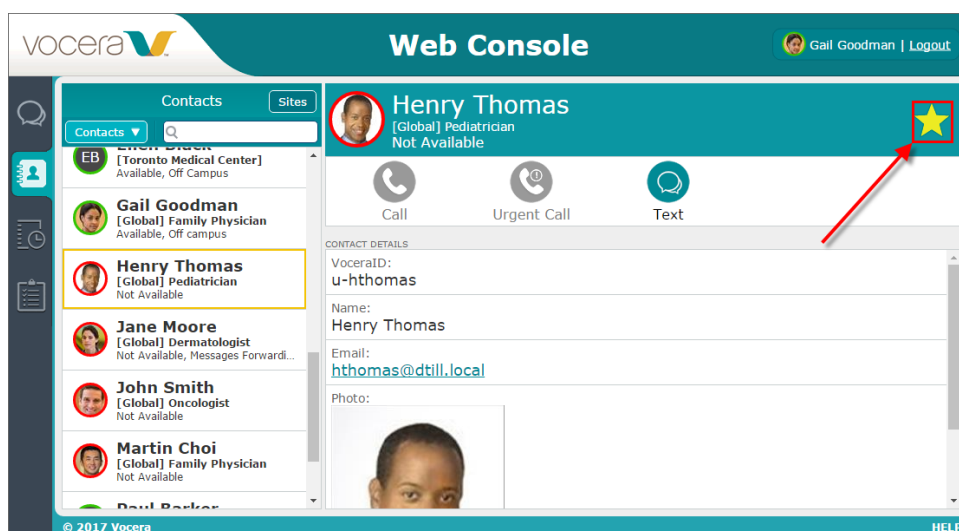


2. Select Contacts at the top of the Contacts pane to display all contacts.
3. Select a contact from the displayed list.



Tip: Start typing the contact name in the search box to quickly find a user or group.

4. Click the star icon located at the top right of the contact. This changes the star to yellow, which marks this contact as a Favorite. The VMP Web Console adds the contact to the Favorites list.



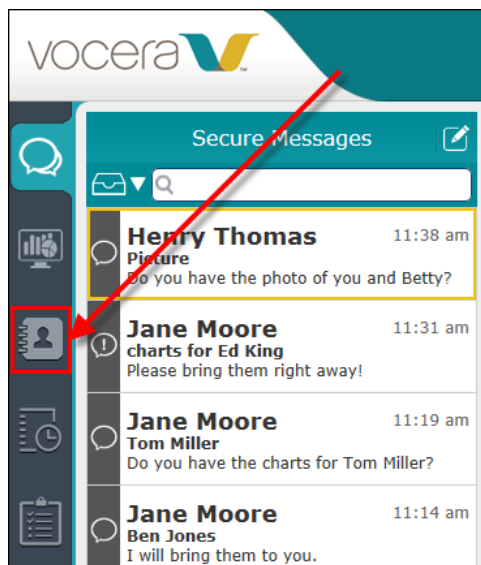
Displaying Contacts in Sites

If contacts have been organized into sites, you can specify which sites are to be displayed in the Contacts list.

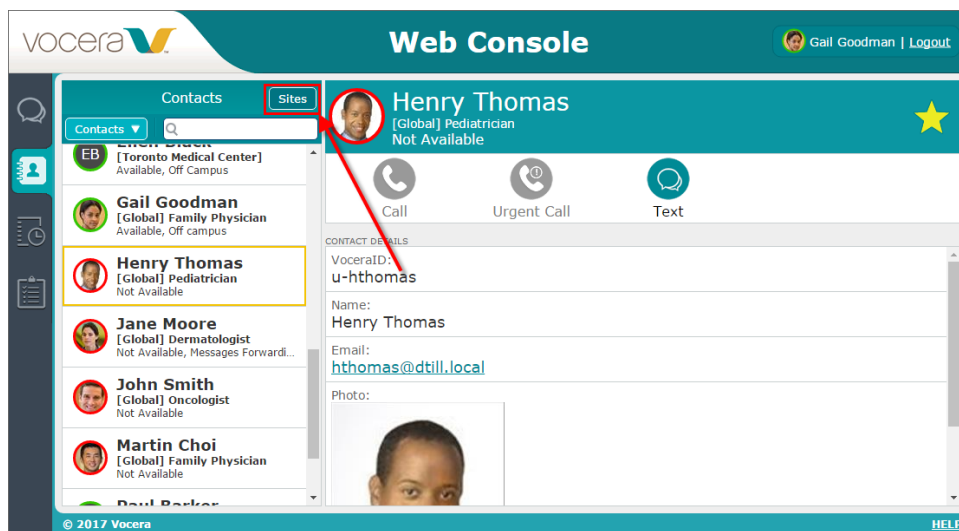


Note: Sites are available if they have been created on the Vocera Voice Server with which the VMP Server has been integrated. See [Vocera Voice Server Integration](#) on page 30 for more information on integrating with the Vocera Voice Server.

1. Click Contacts to display the Contacts view.



2. Click Sites.

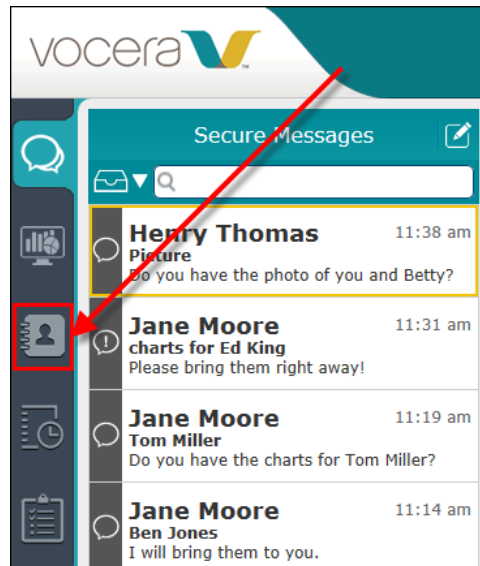


3. In the list of sites that appears, select or clear the sites to display.

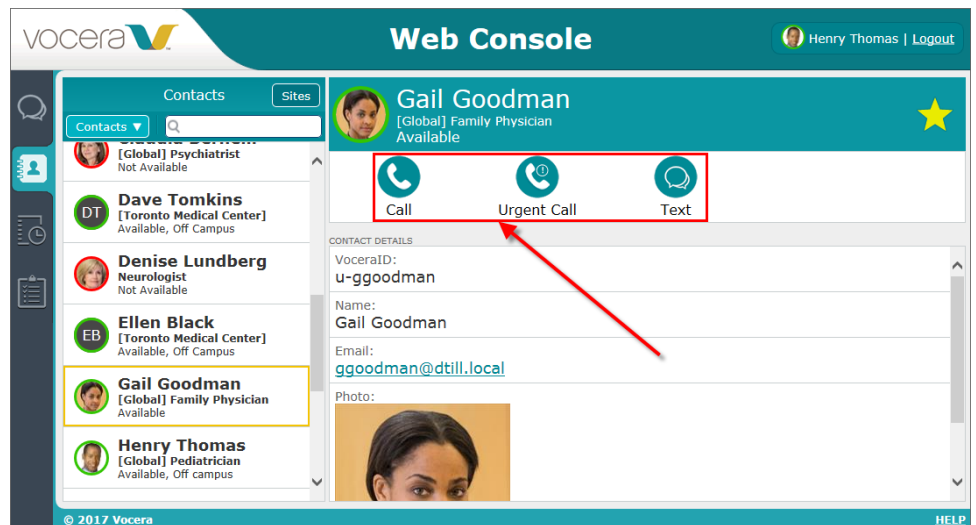
Calling a Contact

If you are logged in to the Vocera Collaboration Suite, you can call a contact from the VMP Web Console.

1. Log on to the VMP Web Console from your Web browser.
2. Click **Contacts** to display the Contacts view.



- Click the name of the contact to which you want to place a Call. The screen for this contact displays the ways that you can communicate with the contact.

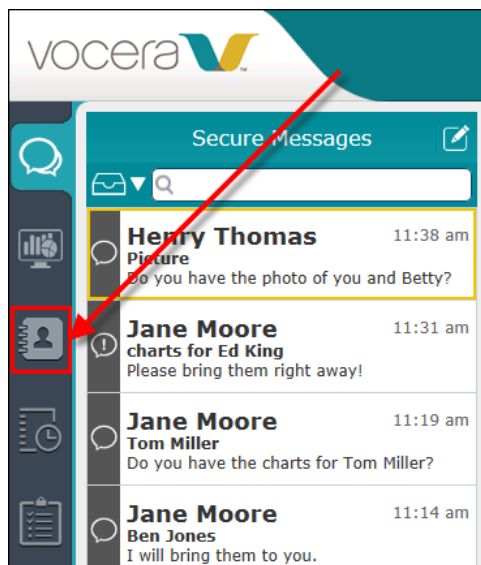


- Click **Call** to place a call to the contact, or click **Urgent Call** to place an urgent call to the contact. This call behaves exactly as if you had originated it from the device.

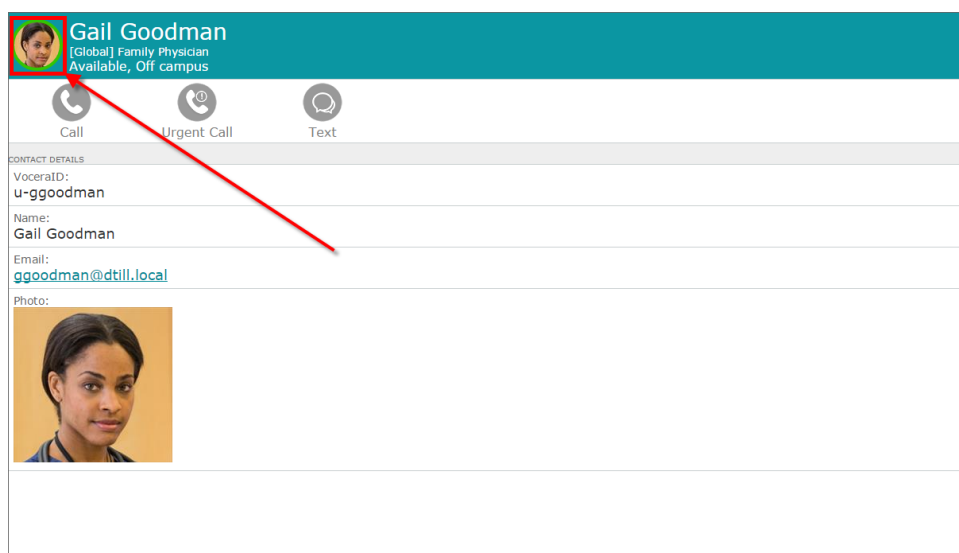
Changing Your Profile Picture

When you are logged in to the VMP Web Console, you can change your profile picture.

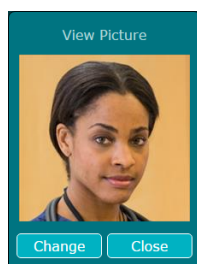
- Log on to the VMP Web Console from your Web browser.
- Click **Contacts** to display the Contacts view.



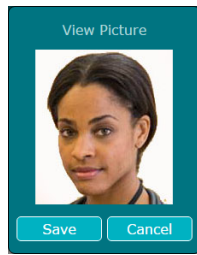
3. Click your name to display your contact page.
4. Click on your profile picture at the top left of the contact page.



5. In the View Picture dialog box that appears, click **Change**.



6. In the file browser window that appears, select the profile picture that you want to use and click **Open**.
7. When the View Picture dialog box reappears, click **Save** to update your profile picture.



Appendixes

These appendixes provide additional reference information that may be useful to you.

VMP Administrator Configuration Options


You can set configuration options to control the behavior of the VMP Administrator.

These options are organized into categories, and some categories are divided into subcategories. To access these options, start the VMP Administrator and select **Configuration > System Options**.



Table 35: System and Networking

Option	Description
<i>Networking</i>	
Vocera Messaging Server Public Host Name / IP	The IP address or fully qualified domain name (friendly DNS name) that devices use to connect to the VMP Server.
Vocera Messaging Server Internal Host Name / IP	The VMP Server IP address used by internal VMP Web Console connections. This can be the same as the public IP address.
<i>Smartphone</i>	

Option	Description
Show integration messages on device lock screen	Whether to allow messages sent from systems integrated with VMP to appear on the lock screens of client devices.  Important: If a message contains confidential patient health information, displaying the message on the lock screen may violate privacy regulations.
<i>Email</i>	
Enable Outgoing Email	Allow outbound email messages to be sent from the VMP Server through SMTP. These include administrative messages and message responses.
Display Name	The name under which outgoing email is to be sent.
Email Address	The email address that outgoing email is to be sent from.
SMTP Server	The SMTP server through which outgoing mail is to be sent.
SMTP Port	The port that the SMTP server uses. The default is 25.
SMTP Authentication	Whether SMTP authentication is required with the SMTP relay host.
<i>Security</i>	
Device Validation Certificate	The approved certificate for device validation. Devices must have installed the corresponding device certificate to be able to access this server.
Enforce SSL for Smartphone connections	Enforce that all communications between the VMP Server and VMP smartphone clients are to use SSL.
Enforce App PIN	Enforce that access to the client application must require PIN entry. Valid settings are OFF, ON, and SHARED (PIN required for shared devices only). This option is set to either SHARED or OFF in the Security Options dialog box during installation - see Installing the VMP Server on page 13 for more details. You can override this setting for any individual user. For more information, see Editing User Information on page 122. If you change the Enforce App PIN setting to ON, device users will not be able to set a PIN if they registered by email or using a registration key and do not have either a valid VMP Server username and password or a valid Active Directory username and password.
App PIN Timeout	If Enforce App PIN has been activated, set the number of seconds that the device can remain idle before the PIN must be re-entered.
Enforce device password for all smartphones	Indicate that the client app is not enabled to run on a device unless a password has been specified for the device. This ensures that sensitive information is kept safe if the device is lost or stolen.
Minimum Password Length	Enter the number of characters the user must include in the device password. For iPhone users, the device Passcode Lock settings must be changed if you want a password longer than 4 numerical digits..
Require at least one letter	Select Yes to ensure that the user adds at least one letter to the device password. For iPhone users, you cannot insist on a password with at least one letter. For iPhone users, the device Passcode Lock settings must be changed if you want a password to include a letter.
Auto Lock	Set the duration of inactivity, in minutes and seconds, until the device auto-locks. In the following example, the device is set to auto-lock after five minutes and thirty seconds: 5m30
Enforce Change Password	Select Yes to ensure the user changes the device password at a regular frequency.
Password Change frequency	If Enforce change password is set to Yes, enter the interval, in days, at which the user is required to change the device password.
Unique passwords before reuse permitted	The VMP Server stores a list of the most recently used passwords for a device. A password cannot be reused if it is one of the <i>N</i> most recent passwords used, where <i>N</i> is the value of this option.
Maximum failed attempts before device wipe	Enter the number of times a password can be incorrectly entered before all system sensitive information is wiped from the device.

Option	Description
Accept client log uploads	Indicates whether log files can be uploaded to the server from Vocera Collaboration Suite clients.
<i>User Inactivity</i>	
Time of inactivity for automatic logout	The number of minutes that the browser and VMP can be inactive before automatic logout. This does not affect clients or the VMP Enterprise Manager.
Days of inactivity before user is placed into Warning state	The number of days before a Warning icon is placed on a user account.
Days of inactivity before user is placed into Locked state	The number of days before an inactive user is locked. This affects both client connections and the VMP Web Console. See Unlocking a User on page 126 for more details.
Time of inactivity for auto logout of smartphone client	The number of minutes that a client can be inactive before automatic logout. Users in Dual Mode are logged out of the smartphone client but not the badge.
Device inactivity timeout interval	If a user is offline for more than the number of minutes specified in this option, the user's status is set to "not available". The maximum value for this option is 1440 minutes (24 hours).
VCS logout in dual mode also causes a badge logout	Whether a user in Dual Mode who logs out of the VCS app should also be automatically logged out of the badge.

Table 36: Contacts

Option	Description
Allow User to upload personal image	Whether a user can upload a photo to their Contact entry from a client application.
Allow Email Communication	This setting controls whether client applications can use email as a mode of communication. If this setting is enabled, the client uses the device's default email editor.

Table 37: Secure Messaging


Option	Description
Enable Remind Me Later Option	Whether to display the <i>Remind Me Later / View Later</i> button when displaying a message on the client application. Message reminders are available for Urgent and High priority messages only, not Normal priority messages.
Default Subject Line for 3rd Party Integrations	The subject line to use when messages are sent from a third-party WCTP source.
Response waiting interval	The number of seconds to wait for a user response when an SNPP or WTCP message is sent.
Retain Message History in Database	The number of weeks that messages are kept in the Microsoft SQL database.
Deliver message content to SMS users	Determines whether the content of an Alert is delivered to an SMS user. The default is No, since SMS channels are non-secure.
Allow Urgent messages	Whether messages can be marked as Urgent.
Include attached images in the report	Whether to include attached images when generating a report
Number of days of inactivity to archive a conversation	The number of days that a conversation is to be inactive before the conversation is archived.
Allow users to forward messages	Whether users can forward messages to another user. Forwarding can also be turned on or off for any specific user.
Forward clinical system messages	Whether to employ user-specified message forwarding settings for messages from clinical systems, including VMI and CWE.  Note: Vocera recommends that you disable this setting, as the behavior is inconsistent when clinical system messages are forwarded to badges.

Table 38: Override Notifications

Option	Description
Enable Do Not Disturb Mode on Smartphone Clients	Whether Do Not Disturb is to be allowed in the client application.


Table 39: Content


Option	Description
Minimum document update frequency	For the Content module, the minimum number of minutes between updates of documents in shared folders.
Allow Content sync with Mapped Network Drives	Whether to support synchronization of Content module documents on mapped network drives (not recommended).

Table 40: Web Console

Option	Description
<i>Disclaimer for Web Logon</i>	
Enabled	Whether a disclaimer popup appears when users log in to the VMP Web Console.
Organization Name	The organization name to appear in the disclaimer popup.
Text	The content of the disclaimer popup.
Web Console Date Format	The format in which dates are displayed in the VMP Web Console.
Enabled	Whether HTML, CSS, and JavaScript static files are sent to the browser in compressed format.

Table 41: Integrations

Option	Description
<i>Vocera Voice</i>	
 Important: If any of these values are changed, you must manually restart the VMP Server. See Starting and Stopping the VMP Server on page 25 for details on how to do this.	
Enabled	Whether the VMP Server is to interact with a Vocera Voice Server.
IP Addresses	The IP address of the Vocera Voice Server, or comma-separated addresses if the Vocera Voice Server is operating in a clustered environment. This option can be set in the Voice Server dialog box during installation. See Installing the VMP Server on page 13 for more details.
Port	The Vocera Voice Server port number.
Use HTTPS	Whether to use HTTPS for secure communication with the Vocera Voice Server.
VCG IP Addresses	The Vocera Client Gateway IP address, or comma-separated addresses if the Vocera Client Gateway is operating in a clustered environment. These addresses are configured when the Vocera Voice Server is installed and has been synchronized with the VMP Server, and cannot be edited here.
VMI Message Expiry	The number of minutes before VMI (Vocera Messaging Interface) messages sent from the Vocera Voice Server expire.
Enable Enhanced Voice Server NIO Tomcat Feature	Whether to enable support for scaling changes included in the Vocera Voice Server. Ensure that this feature is enabled in the Vocera Voice Server before enabling it in the VMP Server.
Use VCG for VCS client connection management	When enabled, the VCS client will use the Vocera Client Gateway server for enhanced connection management. This setting is recommended to improve resource management on the clients. Requires Vocera Client Gateway version 5.2.2 or later and VCS version 3.2 or later. See the <i>Vocera Voice Server Telephony Configuration Guide</i> for details on the VCG properties that configure the VCS and VMP interface.
<i>Patient Context</i>	

Option	Description
Enabled	Set to Yes to enable integration with the Engage Patient Context Adapter.
Adapter URL	The URL of the Engage Patient Context Adapter.
Adapter Authentication Key	The authentication key required to obtain access to the Engage Patient Context Adapter.
<i>AirStrip ONE</i>	
Enabled	Set to Yes to enable integration with the AirStrip ONE platform. This makes it possible for Vocera Collaboration Suite users to obtain access to patient waveform data through an Engage server.
Shared Key	Authenticates the connection between the VMP Server and the AirStrip ONE platform.
Site ID	This ID identifies the connected AirStrip ONE platform.
<i>Vocera Secure Texting App - Message Exchange</i>	
Enabled	Set to Yes to enable messages and images to be exchanged between Vocera Collaboration Suite users and Vocera Secure Texting mobile applications.
User ID	This ID is configured by the VST cloud server to identify the connected Vocera organization.
Shared Key	Authenticates the connection between the VST cloud server and the connected Vocera organization.
<i>Email</i>	
Enable Secure Message Initiation	Enables the configuration of a user's email into the Messaging feature.
<i>Secure Message Initiation - Incoming Mail</i>	
Protocol	The protocol for the mailbox. This is one of POP3, IMAP4, or Exchange Web Services.  Note: SSL connections are supported for IMAP4 and Exchange Web Services only. POP3 does not support SSL connections.
Email Scan Interval	The number of seconds between scans for new incoming email.
Initiation Permitted	Who can initiate messages by email. This is one of the following: <ul style="list-style-type: none"> From any email address: Anyone that can send email can initiate a message. From VMP users only: Only registered VMP users can initiate a message.
EWS Domain	The Exchange Web Services domain. Appears only when Protocol is set to Exchange Web Services.
Email Username	The username associated with the mailbox that the VMP Server is to monitor.
Email Password	The password for the mailbox username.
Confirm Email Password	The password for the mailbox username (repeated).
POP3/IMAP4/EWS Host	The hostname for the server hosting email account. This must be the domain name, not the URL. For example, use mail.customer.com , not https://mail.customer.com/owa .
POP3/IMAP4/EWS Port	The port number for email account connections to the host. See Port Requirements on page 11 for the default port requirements for these protocols.
IMAP4/EWS Use Secure Connection	Whether the connection to the email server must be secured. Appears only when Protocol is set to either IMAP4 or Exchange Web Services.
IMAP4/EWS Security Port	The port number at which the email server is accepting secure connections. See Port Requirements on page 11 for the default secure port requirements for these protocols. Appears only when Protocol is set to either IMAP4 or Exchange Web Services.

Option	Description
IMAP4 Authentication Type	The type of login that the IMAP4 email server supports. Select either <i>Login</i> or <i>Authentication</i> . Appears only when <i>Protocol</i> is set to <i>IMAP4</i> .
IMAP4/EWS Mailbox	The mailbox name to access within the specified email account (for example, <i>Index</i>). Appears only when <i>Protocol</i> is set to either <i>IMAP4</i> or <i>Exchange Web Services</i> .
Delete Email Once Processed	How often the VMP Server will remove emails from the monitored mailbox. This is one of the following: <ul style="list-style-type: none">• <i>Immediately</i>: The VMP Server deletes the email immediately after it has been converted to a message.• <i>Once/Day</i>: The VMP Server deletes all processed emails that are older than 24 hours.• <i>Never</i>: The VMP Server never deletes any email. Select this setting only if email is deleted by another process or person.
WCTP	
PollingID 1	The polling IDs to use when communicating with a WCTP source.
PollingID 2	
PollingID 3	
SMS Aggregation	
Configure SMS aggregator plug-in	Link to the Plugin Configuration window in which you can configure an SMS aggregator service.

Table 42: Scheduling

Option	Description
When does daily validation happen	The time at which schedule validation takes place when it has been specified for on-call schedules. When automatic validation is performed, a report is generated that is emailed to all users that have edit access on the schedule.
Validation look ahead interval	The number of days to look ahead in an on-call schedule when validating. This number can be between 1 and 14.

Table 43: VBI Data Export

Option	Description
Enable VBI Data Export	Whether or not the Vocera Business Intelligence (VBI) Data Export function is active.
Time of Data Export	The time at which to run the VBI Data Export job.
Location of Data Export	Where to store the VBI Data Export logs. The default is the <drive> \Vocera\Support\Upload folder, where <drive> is the drive on which VMP is installed.

VMP Enterprise Manager Configuration Options

From the VMP Enterprise Manager, you can set configuration options to control the behavior of the VMP Server.

These options are organized into categories, and some categories are divided into subcategories. To access these options, start the VMP Administrator and select *Configuration > System Options*.



Options marked with an asterisk * are visible only when you click *Advanced Options*.

If you have installed a standalone version of the VMP Administrator, the VMP Enterprise Manager displays only a limited subset of these options. The options available in a standalone environment are marked with two asterisks **.






Note: If you are using VMP in a clustered environment, you must update these options on each cluster node on which the VMP Server is installed.

Table 44: VMP Enterprise Manager Configuration Options

Option	Description
<i>Database</i>	
<i>Auth</i>	
Login **	The database account used to query stored permissions and authenticate users. The default is wicauth .
Password **	The password for this account.
Confirm Password **	A repetition of the password for this account.
<i>Master</i>	
Login	The account used by the application server and by the VMP Administrator if authenticated successfully. The default is wicapplication .
Password	The password for this account.
Confirm Password	A repetition of the password for this account.
Server **	The IP address of the VMP database server.
MaxConnections * **	The maximum number of cached connections to the SQL server.
DBUpdateFile * **	The SQL file for the DBUpdate tool. This tool is used by Vocera technical support.

Option	Description
<i>Services</i>	
<i>WDE</i>	
NetworkInterface	The IP address of the network interface to which the server listens for requests. If this is set to <code>0.0.0.0</code> , all interfaces are available.
NetworkPort	The HTTP port number for the VMP Server.
NetworkSecurePort	The secure HTTPS port number for the VMP Server.
NetworkSecureCertificate	The SSL certificate to be used with the VMP Server. This is set in the Security Options dialog box during installation. See Installing the VMP Server on page 13 for more details.
NetworkSecureEnforceWebSSL	Enforce the use of SSL when connecting from the VMP Web Console to the VMP Server.
MaxPacketSize *	The data size used by device clients when communicating with the server.
DefaultSliceLimit *	The maximum size of a compressed data chunk in a packet. This enables limiting of memory consumption on the device.
EnableWebServer	Enable the VMP Web Console.
Enable automatic Web login	Enable Active Directory automatic login (supported for Internet Explorer only).
Enable no authentication for Web login	Enable the Open Portal interface.
Do not show VMP instances on Web login page	If multiple instances of the VMP Server are available, do not display them on the VMP Web Console login page.
BISStatusRecordsFlashInterval *	The BIS-B status record expiration interval. This value does not need to be changed.
Apple push protocol version *	This value does not need to be changed.
Apple push idle connection timeout *	This value does not need to be changed.
Google Cloud Messaging project ID *	This value does not need to be changed.
Google Cloud Messaging key *	This value does not need to be changed.
Connection Limit *	The number of requests that the server can handle simultaneously. Requests over the limit are kept in a connection queue.
Connection Timeout *	The length of time that a connection remains in the connection queue.
Media Stream Connections Limit *	The maximum number of simultaneous media streaming HTTP connections.
Device Push Connections Limit *	The maximum number of simultaneous device push connections.
Web Push Connections Limit *	The maximum number of simultaneous web push connections.
Active Directory Server **	The Active Directory IP address or host name when the VMP Server is integrated with Active Directory. This option can be set in the Active Directory dialog box during installation. See Installing the VMP Server on page 13 for more details.
Connect to Active Directory over SSL **	Whether to connect to the Active Directory server using SSL. The default is <code>False</code> .

Option	Description
Allow Active Directory user to login (display login/password form) **	Enable the use of Active Directory user names and passwords when logging into the VMP Administrator. Only users that have been granted permission to log into the VMP Administrator can use their Active Directory credentials. The default is <i>False</i> .
Enable automatic login using Active Directory authentication **	Select <i>True</i> to enable logging into the VMP Web Console using Active Directory credentials. The default is <i>False</i> .
Allow current logged domain user to login (display link) **	Select <i>True</i> to display an auto-login link. If this link is clicked, the VMP Server attempts to automatically log in using Windows authentication. The default is <i>False</i> .
GCMProxy *	This value does not need to be changed.
<i>WCTP</i> *	
Security code *	The security code to allow WCTP polling.
<i>SMTP</i>	
Server	The SMTP server for email notifications. In a clustered environment, this is used to send failover notifications.
Port *	The port number for the SMTP server.
VMP email	The email address that email notifications are sent from.
UseAuthentication *	Whether to use SMTP authentication.
Login *	The login ID for SMTP authentication.
Password *	The password for the SMTP login.
Confirm Password *	A repetition of the password for the SMTP login.
UseSSL *	Whether to use SSL for the SMTP connection.
<i>Network</i> *	
<i>Proxy</i> *	
Enabled *	Whether a proxy is to be enabled on the network. If a proxy is enabled, all outgoing requests go through this proxy.
Host *	The IP address of the proxy.
Username *	The username for the proxy.
Password *	The password for the proxy username.
Confirm Password *	A repetition of the password for the proxy username.
UseSSL *	Whether to use SSL for the proxy.
<i>Soap</i> * **	
ConnectionsLimit * **	The maximum number of simultaneous SOAP connections.
<i>Logging</i>	
Limit log messages to VMP Log File	The levels of log messages to be written to the log file.
Limit log messages to Windows Event Log	The levels of log messages to be written to the Windows event log.
Limit EMail notifications	The levels of log messages for which email notifications are to be sent.
Email Address(es) for Notifications	The email addresses to which email notifications are to be sent.

Option	Description
Enable extended communication logging *	Enables logging of the content of HTTP requests, WCTP, and email. Warning: This logging information may contain message text, which may cause patient-sensitive information to appear in the log files.
Enable smartphone extended communication logging *	Enables logging of VMP smartphone data exchanges.  Warning: This logging information will contain message text.
Enable web console extended communication logging *	Enables logging of VMP Web Console data exchanges.  Warning: This logging information will contain message text.
Enable SOAP extended communication logging *	Enables VMP SOAP interface logging.  Warning: This logging information will contain message text.
Size of log file in megabytes *	Specifies the maximum size of a log file. When the file reaches this size, a new file is started. If 0 is specified, log file rotation is disabled.
Count of log files *	The number of log files to retain in the system. If this is set to 0, log files are never deleted.

Frequently Asked Questions

Answers to commonly occurring problems.

Why am I having issues viewing the VMP Web Console in Internet Explorer (IE) 9?

1. The VMP Web Console URL must be added to the list of trusted sites to work correctly from Internet Explorer 9 or later. For instructions about adding a site to the trusted site list, see: [Microsoft Community - Internet Explorer Question, "How do I add a site to my "trusted sites" list?"](#) If you log into your computer using an Active Directory interface, and therefore do not need to log in to the VMP Web Console to use it, the VMP Web Console URL must be part of the local intranet.
2. To provide the best possible experience while using the VMP Web Console, make sure that you have the Internet Explorer browser set to compatibility mode:
 - a. Open Internet Explorer.
 - b. Press F12.
 - c. Select Browser Mode and ensure it is set to Internet Explorer 9. If you are using a newer browser, set Browser Mode to Internet Explorer 9 Compatibility View.
 - d. Select Document Mode and set it to IE 9 Standards.

Why am I seeing a Fail to Listen error in the logs when the Vocera Data Exchange Service is started?

If your logs list the following error when the Vocera Data Exchange Service is started, another application on the VMP Server is running on port 80:

`Failed to listen on prefix 'http://*:80/' because it conflicts with an existing registration on the machine.`

In most cases, this error occurs because the IIS Service is using port 80. Turn off the IIS World Wide Web Publishing option as described in [Installing the VMP Server](#) on page 13.

My server is no longer pushing communications to iOS devices. What happened?

The APNS certificate must be updated annually. Check with your technical account manager to determine if your certificate requires an update.

For details on how to update an APNS certificate, see [Updating the APNS Certificates](#) on page 76.

Where can I locate the VMP Server logs?

On the VMP Server, locate the drive that VMP is installed on (the default is the C drive), and browse to the following folder:

Program Files/Vocera/WIC/Logs

If your installation of VMP was installed with a version earlier than 5.2.2 and then later upgraded, this folder is:

Program Files/Wallace/WIC/Logs