Vocera Messaging Platform Administration Guide

Version 5.1.0

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: 2018-12-05 06:23

VMP-510-Docs build 267

Contents

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, 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, 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 **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. See **Updating the APNS Certificate** on page 71 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.

VMP Architecture

VMP Messages can be delivered to a number of different devices, including iOS and Android devices running Vocera Collaboration Suite, or to cell phones via SMS. Pagers are also supported using the WCTP and SNPP protocols.

VMP has a SOAP-based API that external systems can use to send messages and receive delivery statuses and responses to the messages. VMP also supports WCTP as an inbound and outbound protocol to allow third-party systems to initiate and receive messages.

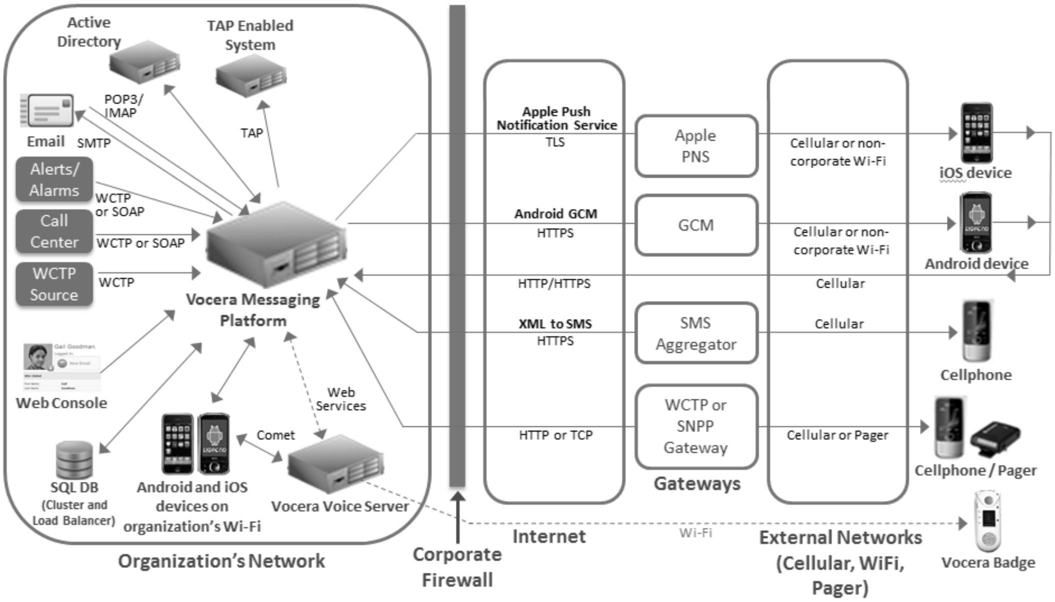


Figure 1: VMP Architecture

Installation

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 **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 **Server Sizing Matrix**.

Network Access Requirements

Prior to installation, make sure 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

To install and deploy the VMP Server, you must have the necessary prerequisites on the installation server.

- A Windows Server that meets the minimum requirements
- The VMP installation files
- The VMP license file
- The SSL certificate that the VMP Server is using, if needed

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

VMP System Accounts

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.

VMP System Settings

The system settings described here must be provided during the VMP installation.

- Public host name or IP address for the VMP Server
- Internal host name or IP address for the VMP Server
- SMTP Settings

Table 3: 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.

Installing the VMP Server

This section provides information about installing the VMP Server.

VMP Server Installation Checklist

Use this checklist to prepare for the VMP installation and deployment.

☐ The VMP installation server meets the minimum server requirements. See **VMP Server Requirements** on page 9.

☐ The VMP software and associated files are available on the installation server. See **VMP Software** on page 9.

☐ The platform minimum network access requirements are available. See **Network Access Requirements** on page 9.

☐ The SQL Server VMP instance is running and meets the minimum requirements. See the **Server Sizing Matrix**.

☐ The Vocera Voice Server is configured to communicate with the VMP Server (if a Vocera Voice Server integration is part of the deployment). See **Vocera Voice Server Integration** on page 26.

☐ The user sources are defined and proper credentials are available to configure the import parameters for remote sources. See **Contacts** on page 83.

Installing the VMP Server

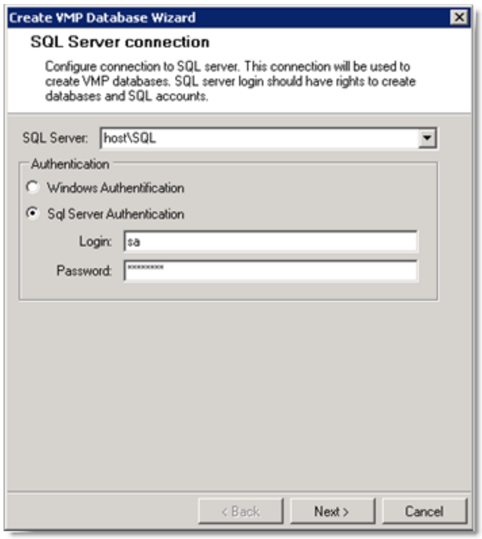
Use these steps to install the VMP Server.

1. 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.
   a. Open the Windows Services application:

    Windows > Start > Administrative Tools > Services
  b. Click to select World Wide Web Publishing Service.
  c. Right-click and select Properties.
  d. From the Startup type dropdown list, select Disabled.
  e. Click Stop, and click Apply.

2. Execute the 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. 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.
7. In the Create VMP Database Wizard dialog, do the following:
   a. 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.



Create VMP Database Wizard

SQL Server connection

Configure connection to SQL server. This connection will be used to create VMP databases. SQL server login should have rights to create databases and SQL accounts.

SQL Server: host\SQL

Authentication

○ Windows Authentification

● Sql Server Authentication

Login: sa

Password: *********

   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 **Server Sizing Matrix**.

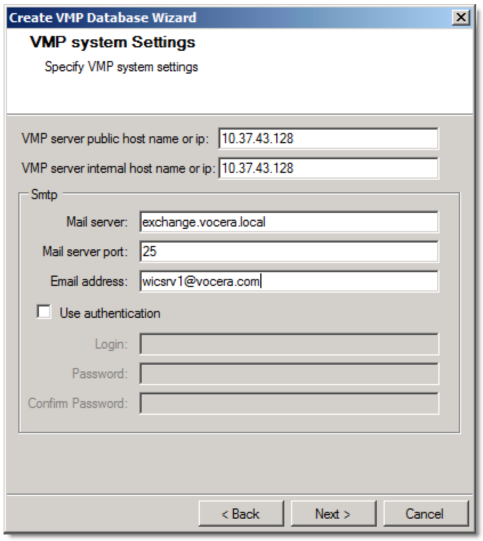
8. Enter a password for the wicapplication and wicauth accounts using the following rules, and click Next.

   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 internal and external host information and the SMTP settings. Click Next.



Create VMP Database Wizard

VMP system Settings

Specify VMP system settings

VMP server public host name or ip: 10.37.43.128

VMP server internal host name or ip: 10.37.43.128

Smtp

Mail server: exchange.vocera.local

Mail server port: 25

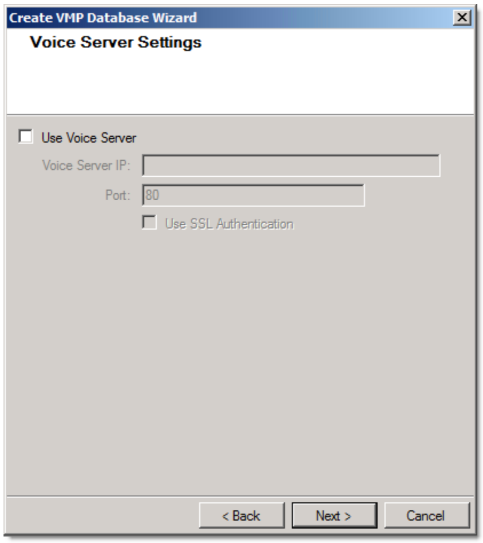
Email address: wicsrv1@vocera.com

☐ Use authentication

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.

Note: For detailed information about System Setting requirements, see **VMP System Settings** on page 10.

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



Create VMP Database Wizard

Voice Server Settings

☐ Use Voice Server

Voice Server IP:

Port: 80

☐ Use SSL Authentication

a. Select Use Voice Server.

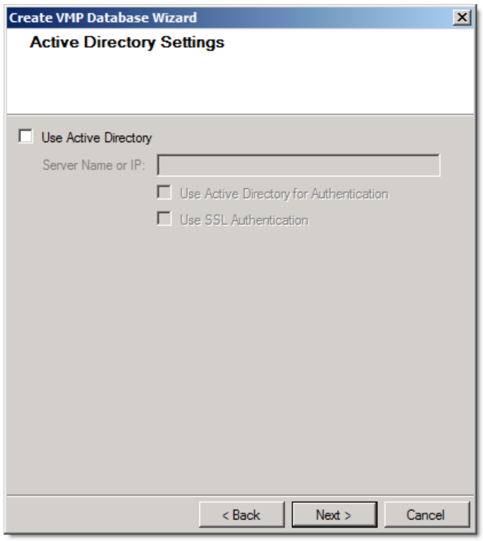
b. In the Voice Server IP field, type the IP address of the Voice server that you want to use. If you are using a clustered environment, ensure that the IP address of the active Voice server is listed first.

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.

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



☐ Use Active Directory

Server Name or IP:

☐ Use Active Directory for Authentication

☐ Use SSL Authentication

a. Select Use Active Directory.

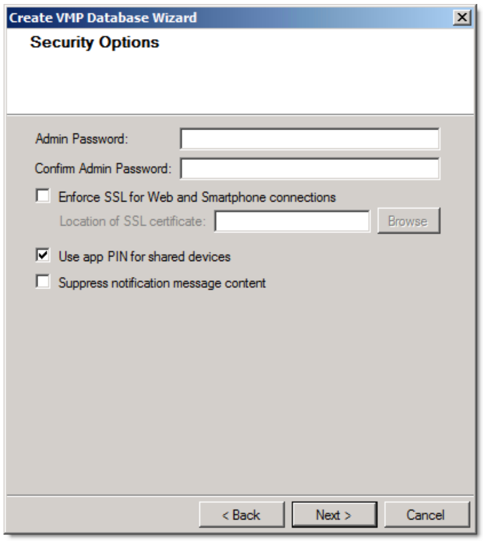
b. In the Server Name or IP field, type the domain name or the IP address of the Active Directory server that you want to use.

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.

12. In the Security Options window:



Admin Password:

Confirm Admin Password:

☐ Enforce SSL for Web and Smartphone connections

Location of SSL certificate:

☑ Use app PIN for shared devices

☐ Suppress notification message content

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 Enforce 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 78 for more details.

f. 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. Skip the step that asks you whether you want to install the `OTA.xml` file.
14. The installer creates the VMP databases on the SQL server. When the script is complete, click OK.
15. This release opens the VMP Enterprise Manager after the database script is complete. Close the application to complete the installation process. Click Finish to close the installer.
16. 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 108.

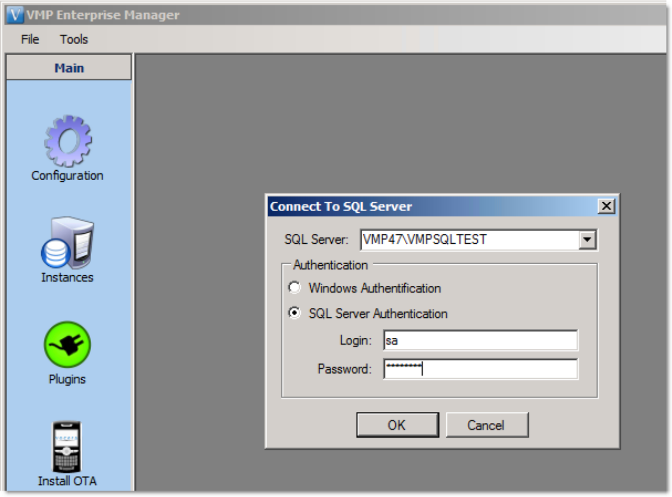
Configuring the VMP License

Use these steps to configure the VMP Server.

1. Start the VMP Enterprise Manager application:

   All Programs > VMP > VMP Enterprise Manager

2. Click the Instances icon and type the SQL Server administrator credentials.



SQL Server: VMP47\VMPSQLTEST

○ Windows Authentification

● SQL Server Authentication

Login: sa

Password: ********

Note: For more information about the SQL Server credential requirements, see the **Server Sizing Matrix**.

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

5. Click OK to close the install dialog.

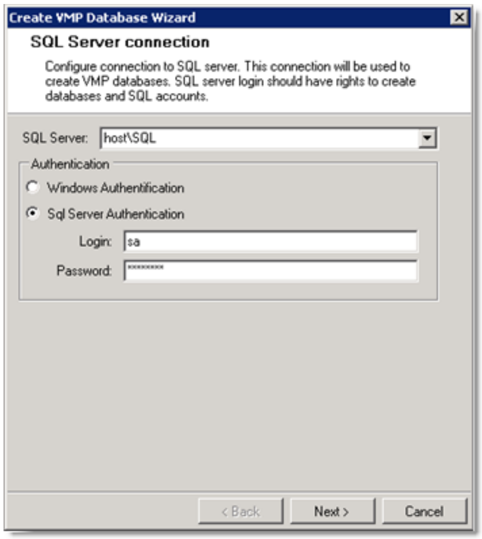
Updating the VMP Server

These steps describe how to install an update of the VMP Server.

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.

1. Stop the Vocera Data Exchange service. See **Starting and Stopping the VMP Server** on page 21 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. 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.



Configure connection to SQL server. This connection will be used to create VMP databases. SQL server login should have rights to create databases and SQL accounts.

SQL Server: host\SQL

○ Windows Authentification

● Sql Server Authentication

Login: sa

Password: ********

    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 **Server Sizing Matrix**.

8. Click OK to confirm that the existing database will be upgraded, and click Next.
9. Skip the step that asks you whether you want to install the `OTA.xml` file.
10. The installer will create 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.

Installing a VMP Cluster

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 **Vocera Messaging Platform Failover** on page 65.

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 10.
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\Wallace\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\Wallace\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 10 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 10.

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.

1. On the first node of the cluster, follow the instructions in **Updating the VMP Server** on page 15 to update the VMP Server.
2. Stop the Vocera Data Exchange Service on the first node. See **Starting and Stopping the VMP Server** on page 21 for details on how to do this.
3. On the second node of the cluster, follow the instructions in **Updating the VMP Server** on page 15 to update the VMP Server.
4. Stop the Vocera Data Exchange Service on the second node.
5. Restart the Vocera Data Exchange Service on the first node of the cluster.

The Smartphone Proxy

To be able to support Active Directory authentication, the VMP Server must be part of the corporate network and must be connected to the domain controller. However, the VMP Server needs to be opened to external traffic, since it needs to communicate with smartphones.

For security reasons, some customers place the VMP Server into a DMZ or perimeter network. Unfortunately, this means that some VMP features, including Active Directory authentication, become unavailable. To solve this problem, the Vocera Smartphone Proxy (VSP) is included with VMP.

The VSP performs the following tasks:

- Accepts HTTP traffic
- Filters smartphone requests
- Authenticates the requests
- Sends the requests to the VMP Server
- Provides replies to the smartphones that sent the requests

The VSP can be installed in the DMZ on a separate server, and will block all traffic to the VMP Server except for authenticated smartphone traffic.

For server requirements for the VSP, see the **Server Sizing Matrix**.

Note: You cannot stream audio and video content to client devices if you are using the VSP to access the VMP Server, since devices are normally connected to the VSP through a cellular network.

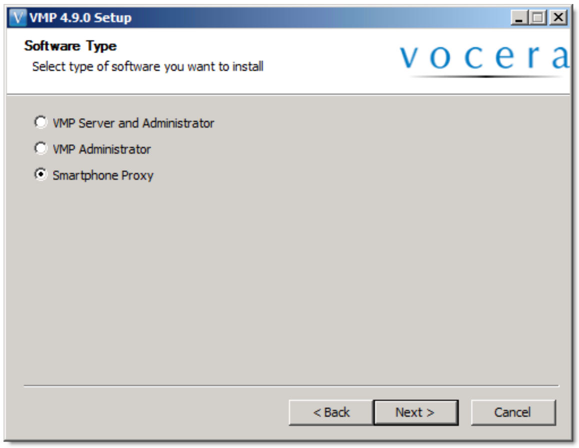
Installing the Vocera Smartphone Proxy (VSP)

The VSP is included as part of the VMP installer, but must be installed as a separate VMP component on a different server.

The VMP Server must be installed first.

To install the VSP:

1. Run `setup.exe`.
2. Select Smartphone Proxy and click Next.



VMP 4.9.0 Setup

Software Type

Select type of software you want to install

- ○ VMP Server and Administrator
- ○ VMP Administrator
- ● Smartphone Proxy

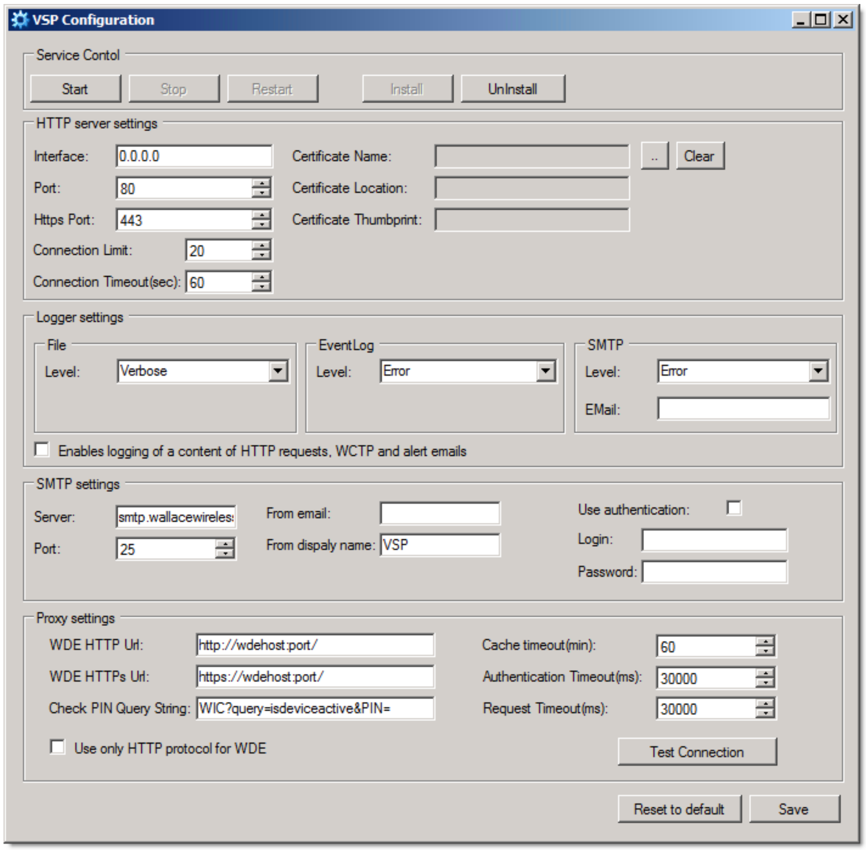
3. Confirm or change the default install location, and click Install.
4. Use the VSP Configuration Utility to configure the proxy settings.
5. Click Save, and click Start.

Note: To uninstall VSP, open the VSP Configuration application, and click Uninstall.

The VSP Configuration Utility

A configuration utility for the VSP is included with VMP.

This utility appears when you install the VSP. It lets you install VSP as a Windows service, start and stop it, and configure it.



VSP Configuration

Service Contol

HTTP server settings

Interface: 0.0.0.0
Port: 80
Https Port: 443
Connection Limit: 20
Connection Timeout(sec): 60
Certificate Name:
Certificate Location:
Certificate Thumbprint:

Logger settings

File Level: Verbose
EventLog Level: Error
SMTP Level: Error
EMail:
☐ Enables logging of a content of HTTP requests, WCTP and alert emails

SMTP settings

Server: smtp.wallacewireles
Port: 25
From email:
From dispaly name: VSP
Use authentication: ☐
Login:
Password:

Proxy settings

WDE HTTP Url: http://wdehost:port/
WDE HTTPs Url: https://wdehost:port/
Check PIN Query String: WIC?query=isdeviceactive&PIN=
Cache timeout(min): 60
Authentication Timeout(ms): 30000
Request Timeout(ms): 30000
☐ Use only HTTP protocol for WDE

Figure 2: The VSP configuration utility

The VSP configuration utility consists of four sections:

- HTTP server settings
- Logger settings
- SMTP settings
- Proxy settings

The HTTP server settings section specifies the network interface that the VSP is listening to.

Table 4: HTTP server settings options

Option	Description
Interface	The IP address for the network interface. Specify 0.0.0.0 to use all available local network interfaces.
Port	The local HTTP port number.
Https Port	The local HTTPS port number.
Connection Limit	The maximum number of simultaneous requests that will be redirected to the application server. This lets you control the impact of smartphone use on the application server load.
Connection Timeout	The number of seconds that the VSP is to keep HTTP requests in the local queue.
Certificate Name, Certificate Location, Certificate Thumbprint	The fields that define the SSL certificate. Click … to browse for the location of a previously installed certificate.

The Logger settings section specifies the settings for file logs, Windows event logs, and log records sent by email.

The SMTP settings section specifies the communication settings for the SMTP server. These settings are identical to the settings specified in the VMP Enterprise Manager.

The Proxy settings section defines the Vocera Data Exchange server that the VSP is connected to. (For historical reasons, this Vocera Data Exchange server is referred to using the initials WDE.)

Table 5: Proxy settings options

Option	Description
WDE HTTP Url	The URL to access the Vocera Data Exchange server using HTTP.
WDE HTTPS Url	The URL to access the Vocera Data Exchange server using HTTPS.
Check PIN Query String	A query to authenticate the device.
Use only HTTP protocol for WDE	Select this checkbox if the VSP is to always use the HTTP interface to communicate with the Vocera Data Exchange server. This lets you use fewer VSP and Vocera Data Exchange resources. If this checkbox is cleared, VSP will use HTTPS if the smartphone requests it.
Cache timeout	The number of minutes that VSP stores information about previously authenticated devices. When the cache record is expired, the VSP re-authenticates the device on the Vocera Data Exchange server.
Authentication Timeout	The number of milliseconds that the VSP will wait for a response from the Vocera Data Exchange server to an authentication request.
Request Timeout	The number of milliseconds that the VSP will wait for a response to an authenticated request redirected to the Vocera Data Exchange server.

VSP High Availability

For best results when implementing a high-availability solution using multiple instances of VSP, implement a round-robin solution with online-offline status using a load balancer.

- The load should be distributed evenly between available VSP instances.
- The VSP instances should all point to the VMP Server, or to an internal VMP load balancer if VMP has been implemented in a cluster deployment.

If you are implementing the Vocera Smartphone Proxy in a high-availability solution, these tests will be of use to you.

- `http://<serverid>/vsptest`: This query checks the status of the VSP.
- `http://<serverid>/WIC?query=test`: This query is terminated on the VMP Server, and tests the status of VMP and the connection between the VSP and the VMP Server.

`<serverid>` is the VSP IP address or domain name. The interval between tests using `http://<serverid>/WIC?query=test` should be identical to the timeout interval on the VSP (this is normally 30 seconds).

If two consecutive queries fail on a particular instance of VSP:

- This VSP instance should be considered unavailable.
- The load balancer should route traffic to the other available VSP instances.
- An email notification should be sent to the administrator, along with the results of the `http://<serverid>/vsptest` query. If this query fails, this VSP service is down and should be considered offline, and the administrator needs to attend to the server (for example, restart the server or start up the virtual machine). If this query passes, it may indicate that either the VMP Server is unavailable or the connection to it is unavailable. In this case, the administrator should look at the VMP Server or the connection between it and the VSP.

`http://<serverid>/WIC?query=test` queries should continue. If a query passes, this instance of VSP is again functional and can be considered online. The load balancer should redistribute loading to this VSP instance.

Note: Optional smartphone URL filtering on the external load balancer can reduce loading on the VSP instances.

Deploying VMP

Learn how to deploy VMP in your environment, including how to import and add users and contacts, how to encrypt your data for greater security, and how to deploy a failover environment to ensure maximum reliability.

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.

VMP Server Log Files

The VMP Server log files provide information on all actions performed by the VMP Server. This can be useful if an unexpected error occurs.

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\Wallace\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, and scroll down to the Logging section.
3. 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 6: 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.

Option	Description
Errors	Write only errors to the log files.

4. 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 **Vocera Messaging Platform Failover** on page 65.

Configuring Wireless Gateways

The wireless gateways listed here can be configured for VMP.

- SNPP
- WCTP Connections

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.

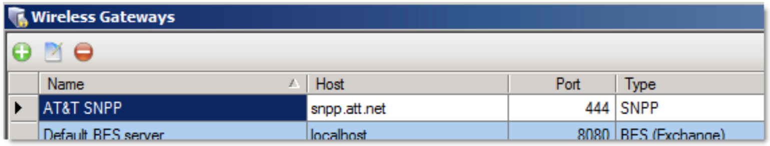
For a list of provider SNPP addresses and port numbers, see **Note Page - Simple Network Paging Protocol (SNPP)**.

Configuring an SNPP Wireless Gateway

For a deployment with SNPP protocol, use these steps to configure the SNPP Wireless Gateway in the VMP Administrator.

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



Name	Host	Port	Type
AT&T SNPP	snpp.att.net	444	SNPP
Default BES server	localhost	8080	BES (Exchange)

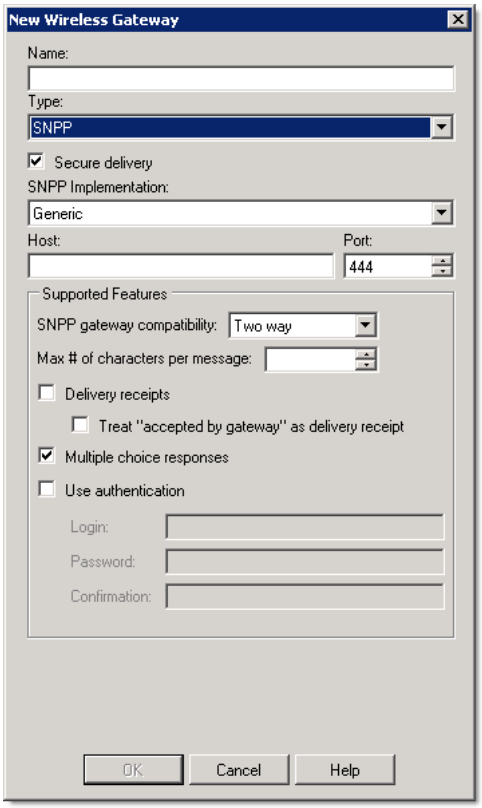
5. Select the SNPP Implementation from the dropdown list.

   ATT, Sprint, and Verizon are pre-configured. For another implementation, select Generic and provide the following details:

Table 7: 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.

Option	Values
Port	Specify the port number to use.
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.



Name:

Type: SNPP

☑ Secure delivery

SNPP Implementation: Generic

Host:

Port: 444

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:

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 Emergin
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.

Table 8: User profile override tags

Tag	Description
OverrideProfileIfHigh=Y	Override user profile when priority is **high**.
OverrideProfileIfNormal=Y	Override user profile when priority is **normal**.
OverrideProfileIfLow=Y	Override user profile when priority is **low**.

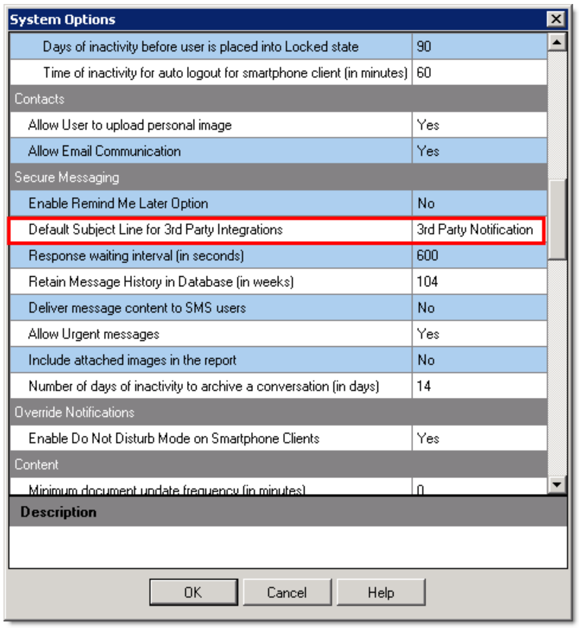
Note: These settings are supported on the Vocera Collaboration Suite and other Vocera smartphone clients.

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.
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.

   Note: To synchronize this user with the WCTP source, set the Pager ID field for this user to match the WCTP Source `senderID`.
5. Click Next, and click Finish.
6. Select Configuration > System Options.
7. Scroll down to the Default Subject for 3rd Party Integrations entry, change the subject line as appropriate for your deployment, and click OK.



Days of inactivity before user is placed into Locked state	90
Time of inactivity for auto logout for smartphone client (in minutes)	60
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	No
Allow Urgent messages	Yes
Include attached images in the report	No
Number of days of inactivity to archive a conversation (in days)	14
Override Notifications	
Enable Do Not Disturb Mode on Smartphone Clients	Yes
Content	
Minimum document update frequency (in minutes)	0

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. Navigate to the Users view:

   Users & Groups > Users

3. Click to highlight the a user entry, and click Edit
4. Enter a value in the Pager ID field to match the WCTP Source `recipientID`.

   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.

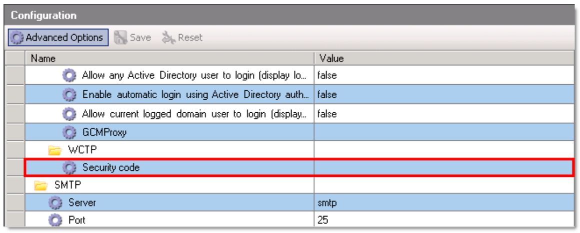
5. Click Next, and click Finish.

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 Enterprise Manager: Start > All Programs > VMP >VMP Enterprise Manager
2. Select Configuration and click Advanced Options.
3. Scroll down to WCTP and enter a Security Code.



Name	Value
Allow any Active Directory user to login (display lo...	false
Enable automatic login using Active Directory auth...	false
Allow current logged domain user to login (display...	false
GCMProxy	
WCTP	
Security code	
SMTP	
Server	smtp
Port	25

Note: If a valid security code is not provided, a WCTP request is rejected with a WCTP 402 error.

4. Click Save.
5. Click OK to confirm the saved settings, and click Yes to restart the server.
6. Start the VMP Administrator.
7. Open the System Options view: Configuration > System Options
8. Scroll down to WCTP, enter the polling IDs, and click OK.

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 9: Vocera Voice Server configuration requirements

Configuration Requirement	Description
Vocera Voice Server Software Requirements	Vocera Voice Server version 4.4.1 or later. If you are synchronizing Vocera Voice Server departments with VMP groups, you require Vocera Voice Server version 5.1 or later.
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:

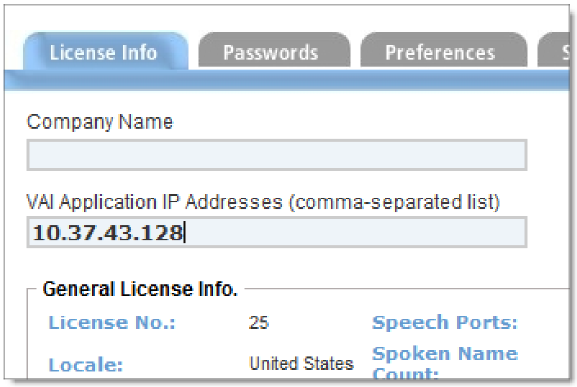
- Vocera Client Gateway: required for Wi-Fi calling

- Vocera SIP Telephony Gateway: required for cellular calling

Vocera Voice Server and VMP Configuration

Use these steps to configure the Vocera Voice Server and VMP to work together.

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.



Company Name

VAI Application IP Addresses (comma-separated list)

10.37.43.128

General License Info.

License No.: 25

Speech Ports:

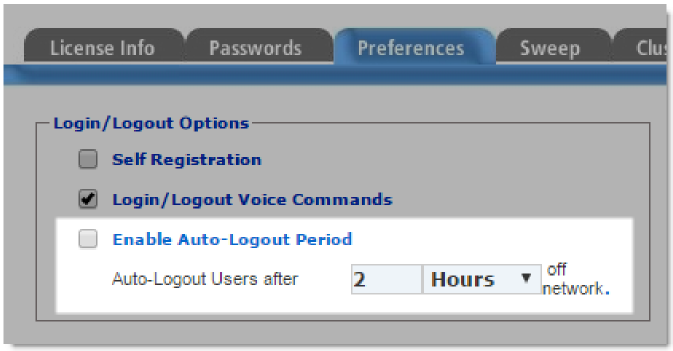
Locale: United States

Spoken Name Count:

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

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.



Login/Logout Options

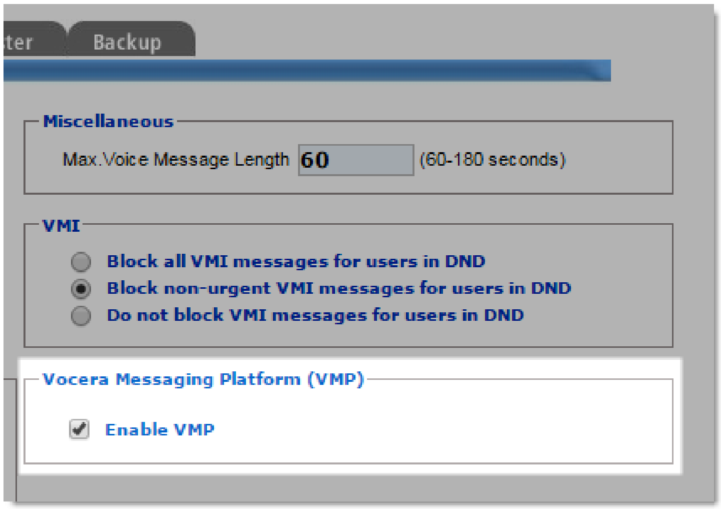
☐ Self Registration

☑ Login/Logout Voice Commands

☐ Enable Auto-Logout Period

Auto-Logout Users after 2 Hours off network.

9. Select the Enable VMP checkbox.



Miscellaneous

Max.Voice Message Length 60 (60-180 seconds)

VMI

○ Block all VMI messages for users in DND
● Block non-urgent VMI messages for users in DND
○ Do not block VMI messages for users in DND

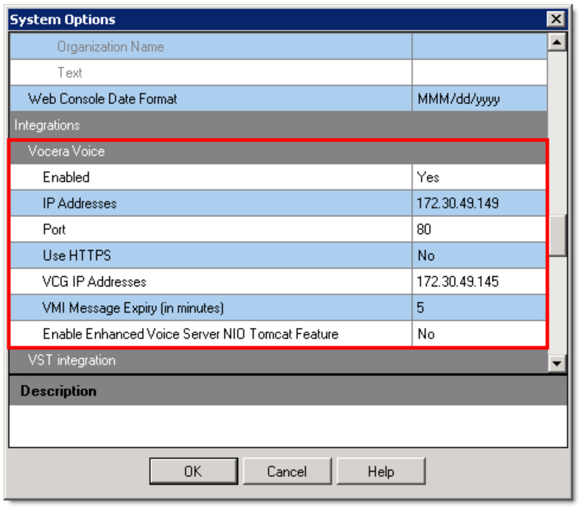
Vocera Messaging Platform (VMP)

☑ Enable VMP

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



Organization Name	
Text	
Web Console Date Format	MMM/dd/yyyy
Integrations	
Vocera Voice	
Enabled	Yes
IP Addresses	172.30.49.149
Port	80
Use HTTPS	No
VCG IP Addresses	172.30.49.145
VMI Message Expiry (in minutes)	5
Enable Enhanced Voice Server NIO Tomcat Feature	No
VST integration	

Description

15. Enter the following values:

Table 10: 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 10 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.

Option	Value
Port	Enter the Vocera 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.

Important: If any of these settings change, you must manually restart the VMP Server. See **Starting and Stopping the VMP Server** on page 21 for details on how to do this.

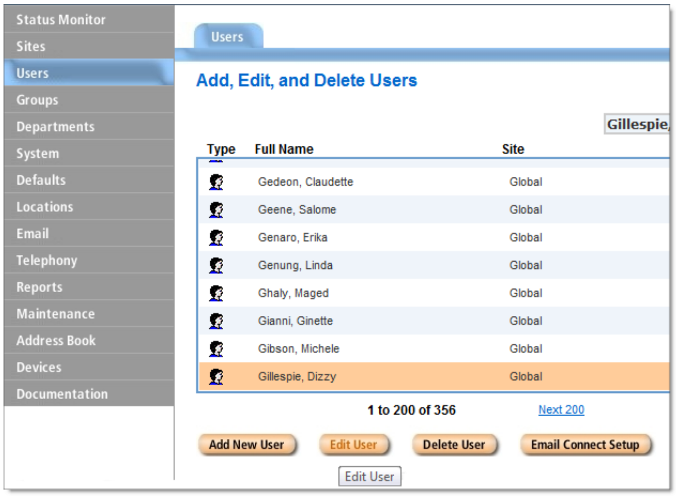
16. Click OK to save your changes.

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 Vocera Voice Server Contacts** on page 36 for information.

Enabling a Vocera Voice User for VMP Paging

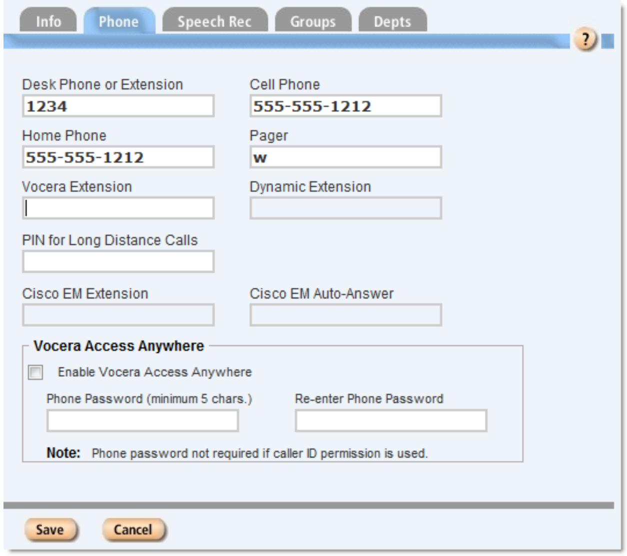
You can use the Vocera Voice Server Administration Console to enable a Vocera Voice user for VMP paging.

1. From the Vocera Voice Server Administration Console, select Users, click to highlight the desired user, and click Edit User.



Type	Full Name	Site
👤	Gedeon, Claudette	Global
👤	Geene, Salome	Global
👤	Genaro, Erika	Global
👤	Genung, Linda	Global
👤	Ghaly, Maged	Global
👤	Gianni, Ginette	Global
👤	Gibson, Michele	Global
👤	Gillespie, Dizzy	Global

2. Click the Phone tab, type the letter `w` in the Pager text field, and click Save.



Desk Phone or Extension: 1234

Cell Phone: 555-555-1212

Home Phone: 555-555-1212

Pager: w

☐ Enable Vocera Access Anywhere

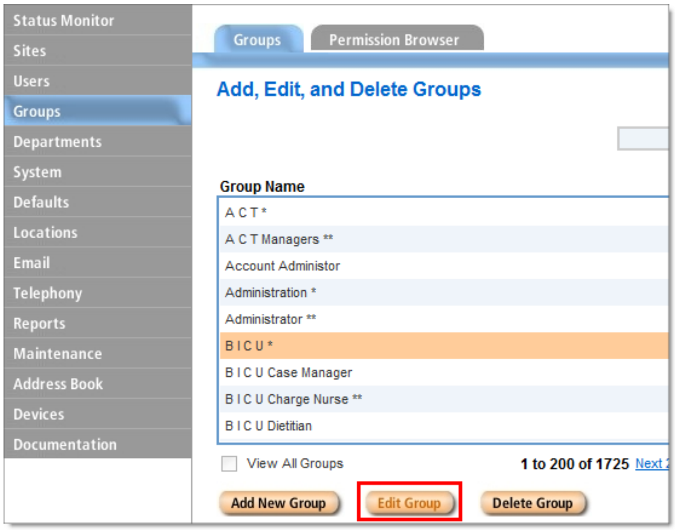
Note: Phone password not required if caller ID permission is used.

Note: The VMP Server sends a message to the user's smartphone (not the badge).

Configuring Groups for VMP Paging

You can use the Vocera Voice Server Administration Console to configure a group for VMP paging.

1. From the Vocera Voice Server Administration Console, select Groups, click to highlight the desired group, and click Edit Group.



Add, Edit, and Delete Groups

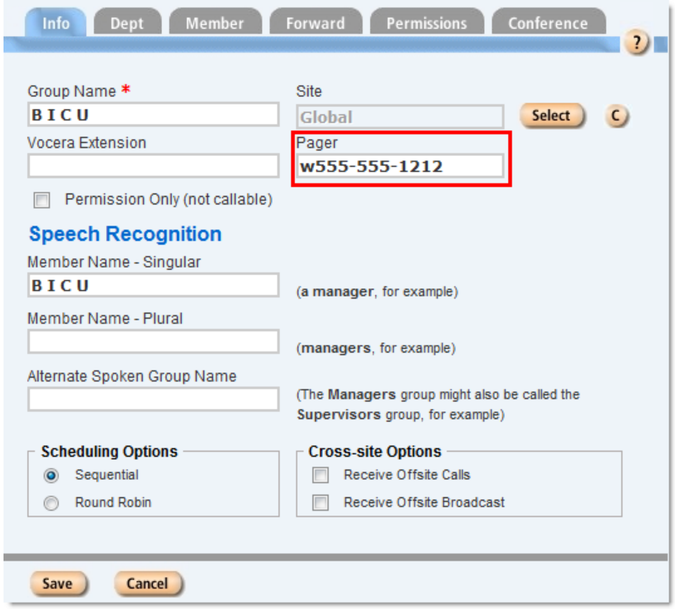
Group Name

A C T *
A C T Managers **
Account Administor
Administration *
Administrator **
B I C U *
B I C U Case Manager
B I C U Charge Nurse **
B I C U Dietitian

☐ View All Groups

1 to 200 of 1725 Next

2. In the Info tab, in the Pager field, type the letter `w` followed by a unique set of numbers, and click Save.



Group Name *
BICU

Site
Global

Vocera Extension

Pager
w555-555-1212

☐ Permission Only (not callable)

Speech Recognition

Member Name - Singular
BICU
(a **manager**, for example)

Member Name - Plural
(**managers**, for example)

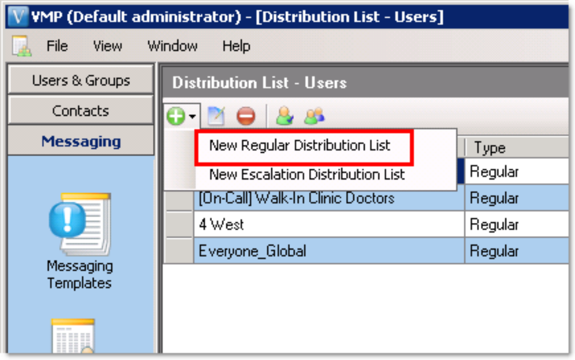
Alternate Spoken Group Name
(The **Managers** group might also be called the **Supervisors** group, for example)

Scheduling Options
● Sequential
○ Round Robin

Cross-site Options
☐ Receive Offsite Calls
☐ Receive Offsite Broadcast

3. From the VMP Server, open the VMP Administrator and select Messaging > Distribution Lists .

4. Click New > New Regular Distribution List.

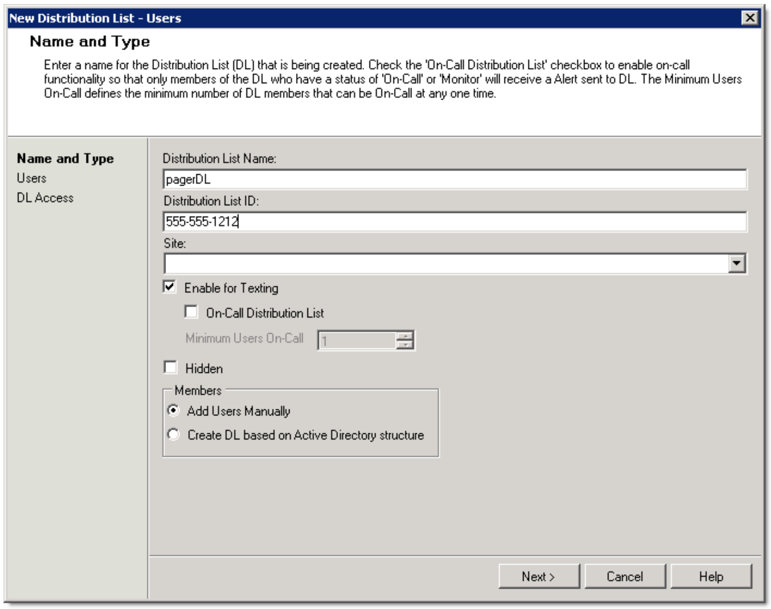

VMP (Default administrator) - [Distribution List - Users]
File
View
Window
Help
Users & Groups
Contacts
Messaging
Messaging Templates
Distribution List - Users
New Regular Distribution List
New Escalation Distribution List

	Type
	Regular
[On-Call] Walk-In Clinic Doctors	Regular
4 West	Regular
Everyone_Global	Regular

5. Type a name in the Distribution List Name box.

6. Type the pager ID in the Distribution List ID box.

Note: This must be the pager ID entered in the Vocera Voice Server Group profile.



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.

Distribution List Name: pagerDL

Distribution List ID: 555-555-1212

Site:

☑ Enable for Texting

☐ On-Call Distribution List

Minimum Users On-Call 1

☐ Hidden

Members

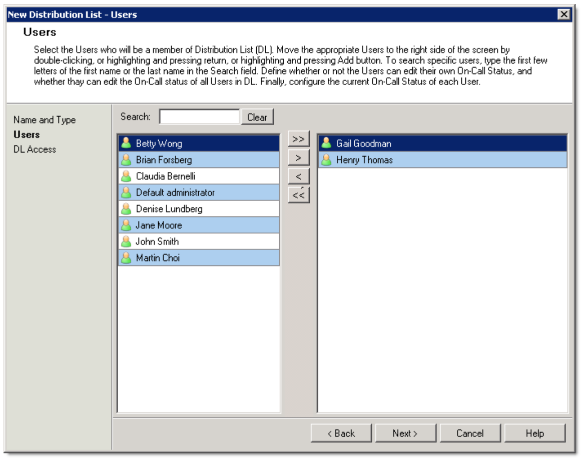
● Add Users Manually

○ Create DL based on Active Directory structure

7. Optionally select a site for the group from the Site dropdown list.

   Note: Sites are defined in the Vocera Voice Server Administration Console.

8. Click Next.
9. Click to highlight the DL users (CRTL + click to select more than one user), click > to add the users to the list, and click Next.

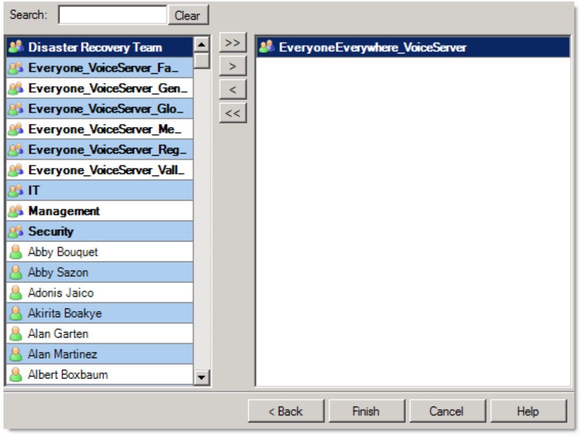


Select the Users who will be a member of Distribution List (DL). Move the appropriate Users to the right side of the screen by double-clicking, or highlighting and pressing return, or highlighting and pressing Add button. To search specific users, type the first few letters of the first name or the last name in the Search field. Define whether or not the Users can edit their own On-Call Status, and whether thay can edit the On-Call status of all Users in DL. Finally, configure the current On-Call Status of each User.

Betty Wong
Brian Forsberg
Claudia Bernelli
Default administrator
Denise Lundberg
Jane Moore
John Smith
Martin Choi

Gail Goodman
Henry Thomas

10. Click to highlight the VMP users who can see and use the DL (CTRL + click to select more than one user), click > to add the users to the list, and click Finish.


Search:
Clear
Disaster Recovery Team
Everyone_VoiceServer_Fa...
Everyone_VoiceServer_Gen...
Everyone_VoiceServer_Glo...
Everyone_VoiceServer_Me...
Everyone_VoiceServer_Reg...
Everyone_VoiceServer_Vall...
IT
Management
Security
Abby Bouquet
Abby Sazon
Adonis Jaico
Akirita Boakye
Alan Garten
Alan Martinez
Albert Boxbaum
>>
>
<
<<
EveryoneEverywhere_VoiceServer
< Back
Finish
Cancel
Help

Enabling Enhanced Vocera Voice Server NIO Tomcat Support

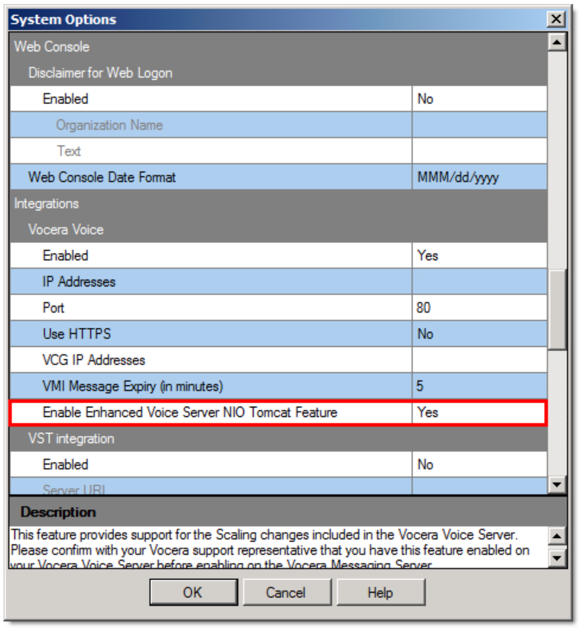
If your Vocera Voice Server has enabled Non-Blocking I/O (NIO) connectivity with Tomcat, you can configure VMP to use it.

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



Web Console	
Disclaimer for Web Logon	
Enabled	No
Organization Name	
Text	
Web Console Date Format	MMM/dd/yyyy
Integrations	
Vocera Voice	
Enabled	Yes
IP Addresses	
Port	80
Use HTTPS	No
VCG IP Addresses	
VMI Message Expiry (in minutes)	5
Enable Enhanced Voice Server NIO Tomcat Feature	Yes
VST integration	
Enabled	No
Server URI	

Description

This feature provides support for the Scaling changes included in the Vocera Voice Server. Please confirm with your Vocera support representative that you have this feature enabled on your Vocera Voice Server before enabling on the Vocera Messaging Server.

5. Click OK to save your change.

Creating Vocera Collaboration Suite Users

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.

Exporting Address Book Entries to the Vocera Voice Server

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.

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:

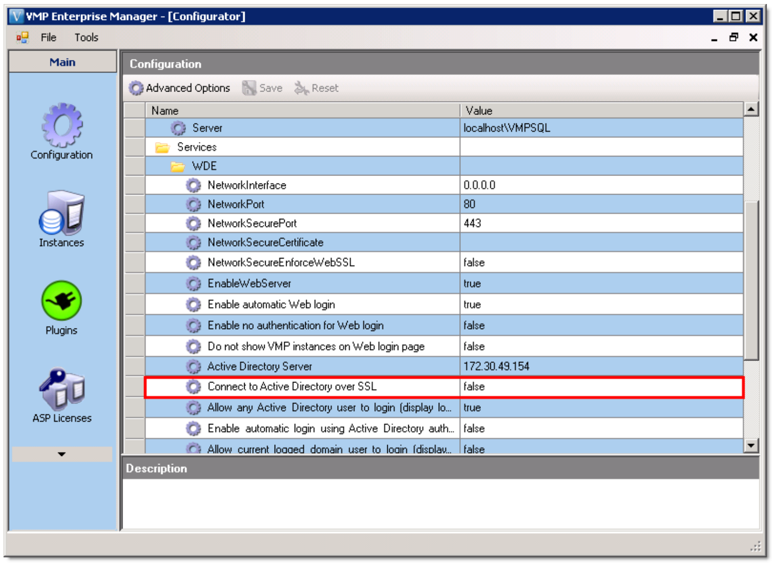
- You can configure the VMP Server to interact with Active Directory using an SSL connection.
- You can allow users to log into the VMP Administrator or VMP Web Console using their Active Directory username and password, provided you have granted permission to these users.

Note: See **Editing User Information** on page 78 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

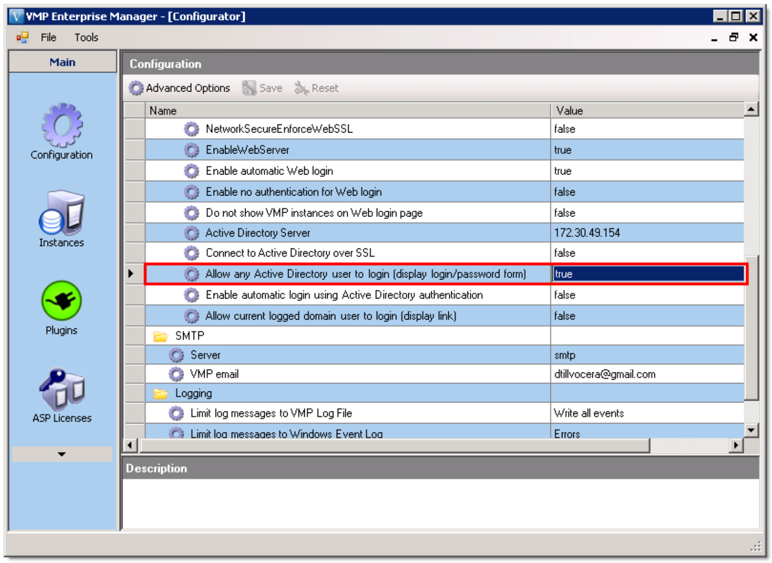
2. Click the Configuration icon.
3. If you want to use SSL with Active Directory, scroll down to the Connect to Active Directory over SSL field.



Name	Value
Server	localhost\VMPSQL
Services	
WDE	
NetworkInterface	0.0.0.0
NetworkPort	80
NetworkSecurePort	443
NetworkSecureCertificate	
NetworkSecureEnforceWebSSL	false
EnableWebServer	true
Enable automatic Web login	true
Enable no authentication for Web login	false
Do not show VMP instances on Web login page	false
Active Directory Server	172.30.49.154
Connect to Active Directory over SSL	false
Allow any Active Directory user to login (display lo...	true
Enable automatic login using Active Directory auth...	false
Allow current logged domain user to login (display...	false

Set this value to true.

4. 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, scroll down to the Allow any Active Directory user to login (display login/password form) field and set it to true.



Name	Value
NetworkSecureEnforceWebSSL	false
EnableWebServer	true
Enable automatic Web login	true
Enable no authentication for Web login	false
Do not show VMP instances on Web login page	false
Active Directory Server	172.30.49.154
Connect to Active Directory over SSL	false
Allow any Active Directory user to login (display login/password form)	true
Enable automatic login using Active Directory authentication	false
Allow current logged domain user to login (display link)	false
SMTP	
Server	smtp
VMP email	dtillvocera@gmail.com
Logging	
Limit log messages to VMP Log File	Write all events
Limit log messages to Windows Event Log	Errors

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

Importing and Synchronizing Users and Contacts

The VMP Server synchronizes with other servers to import the platform user and contact base.

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.

Import options include:

- Active Directory: see **Importing Active Directory Users** on page 39
- Vocera Server: see **Importing Vocera Voice Server Contacts** on page 36
- Excel and CSV files: see **Synchronizing With an Excel or CSV File** on page 45
- SQL: see **Synchronizing With SQL** on page 48

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

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

Tip: Before building a user base from imported sources, plan the source field mappings needed for your environment. Field mappings can be configured for users and for contacts. For details about source field mapping, see **Editing User Fields** on page 105 and **Defining Contact Fields** on page 104.

Note: Synchronize new imports with existing contacts to ensure the maintenance and update of contacts is uninterrupted and all system contacts stay up to date.

Importing Vocera Voice Server Contacts

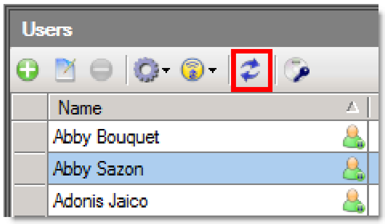
If you plan to integrate the VMP Server with a Vocera Voice Server, you must import the Vocera Voice Server contacts into the VMP Server.

Note: See **Vocera Voice Server Integration** on page 26 for information on integrating the VMP Server with a Vocera Voice Server.

Important: Before beginning a Vocera Voice Server import, make sure each user email address is entered on the Vocera Voice Server. The email address is used to match VMP source users from other imports and prevent duplicate user entries. Make sure the paging field in the Vocera Voice Server user profile is blank. This field is mapped on the VMP Server.

1. Start the VMP Administrator:

   All Programs >VMP>VMP Administrator
2. Type `admin` in the VMP Login dialog, and click OK.
3. Select Users & Groups > Users.
4. Click the Synchronization icon in the Users view.



Users

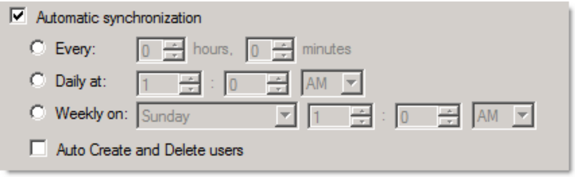
Name

Abby Bouquet

Abby Sazon

Adonis Jaico

5. In the Reconfigure/Synchronize only window, select Yes, reconfigure settings. Click Next.
6. Configure the Automatic synchronization options.



☑ Automatic synchronization

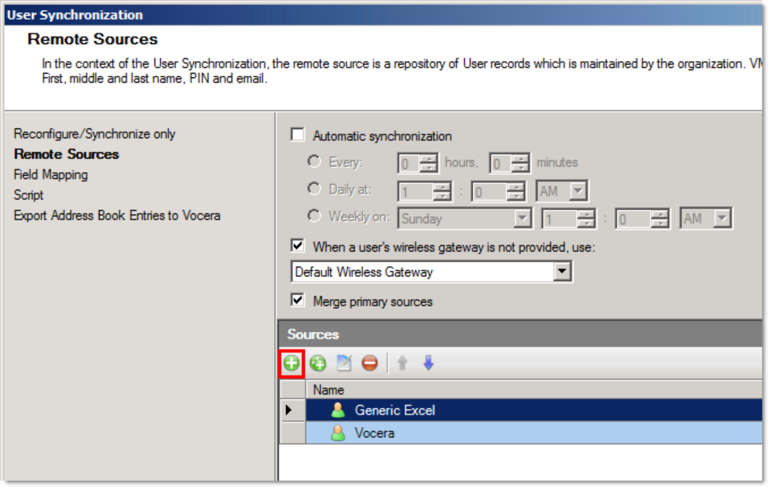
○ Every: 0 hours, 0 minutes

○ Daily at: 1 : 0 AM

○ Weekly on: Sunday 1 : 0 AM

☐ Auto Create and Delete users

7. In the User Synchronization dialog, click the Add primary source with users icon (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. V
First, middle and last name, PIN and email.

☐ Automatic synchronization

○ Every: 0 hours, 0 minutes

○ Daily at: 1 : 0 AM

○ Weekly on: Sunday 1 : 0 AM

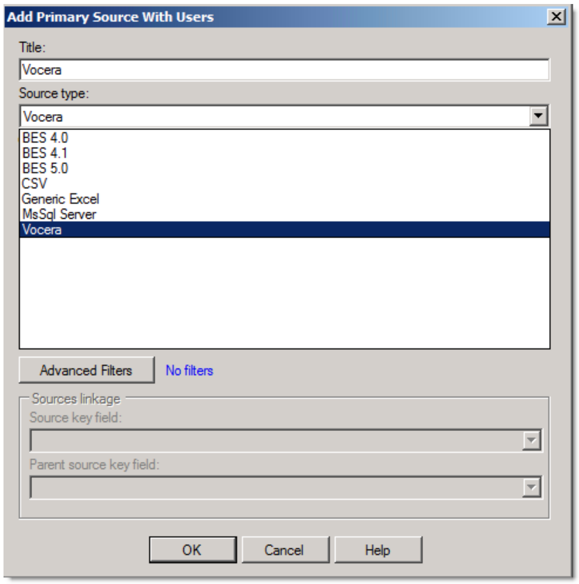
☑ When a user's wireless gateway is not provided, use: Default Wireless Gateway

☑ Merge primary sources

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

8. Select Vocera from the Source type dropdown list, and click OK. This selection auto-populates the Title field. You can accept the default title or customize the title.

   Note: If you have multiple connections, you must repeat this step for each connection.

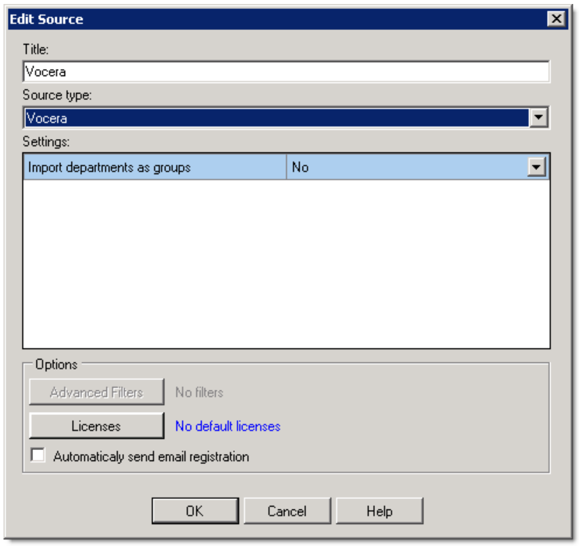


Add Primary Source With Users

Title: Vocera

Source type: Vocera

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



Title: Vocera

Source type: Vocera

Settings:

Import departments as groups	No

Options

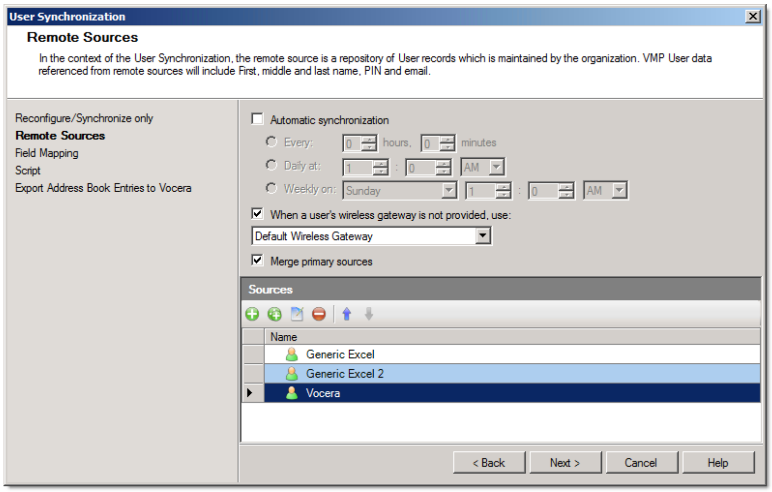
No filters

No default licenses

☐ Automaticaly send email registration

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

10. The Vocera Voice Server source is now configured. Make sure it is highlighted, and click Next in the User Synchronization dialog.



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.

☐ Automatic synchronization

○ Every: 0 hours, 0 minutes

○ Daily at: 1 : 0 AM

○ Weekly on: Sunday 1 : 0 AM

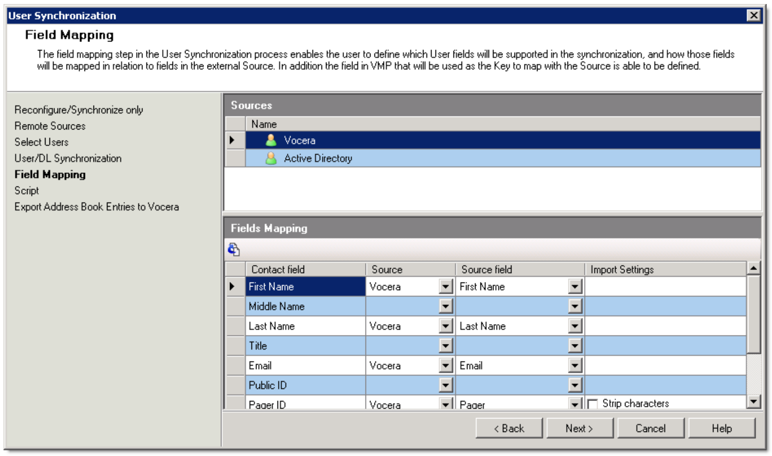
☑ When a user's wireless gateway is not provided, use:

Default Wireless Gateway

☑ Merge primary sources

Name
Generic Excel
Generic Excel 2
Vocera

11. The Field Mapping dialog allows for basic field mapping from the Vocera Source to the VMP user contact. Define the field mappings for your deployment, and click Next.



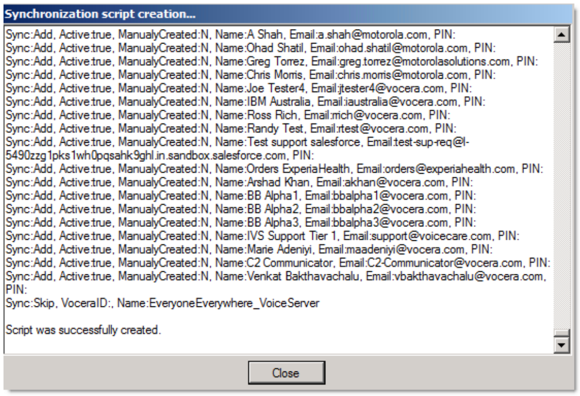
Field Mapping

The field mapping step in the User Synchronization process enables the user to define which User fields will be supported in the synchronization, and how those fields will be mapped in relation to fields in the external Source. In addition the field in VMP that will be used as the Key to map with the Source is able to be defined.

Name
Vocera
Active Directory

Contact field	Source	Source field	Import Settings
First Name	Vocera	First Name	
Middle Name			
Last Name	Vocera	Last Name	
Title			
Email	Vocera	Email	
Public ID			
Pager ID	Vocera	Pager	☐ Strip characters

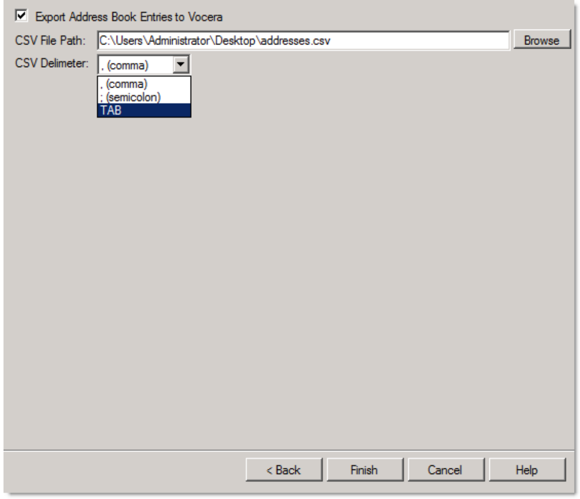
12. The synchronization script generated by the import wizard options is revealed in a script dialog box. Use the scroll bar to review the script and click Close.



```
Sync:Add, Active:true, ManualyCreated:N, Name:A Shah, Email:a.shah@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Ohad Shatil, Email:ohad.shatil@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Greg Torrez, Email:greg.torrez@motorolasolutions.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Chris Morris, Email:chris.morris@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Joe Tester4, Email:jtester4@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:IBM Australia, Email:iaustralia@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Ross Rich, Email:rrich@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Randy Test, Email:rtest@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Test support salesforce, Email:test-sup-req@l-
5490zzg1pks1wh0pqsahk9ghl.in.sandbox.salesforce.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Orders ExperiaHealth, Email:orders@experiahealth.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Arshad Khan, Email:akhan@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha1, Email:bbalpha1@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha2, Email:bbalpha2@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha3, Email:bbalpha3@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:IVS Support Tier 1, Email:support@voicecare.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Marie Adeniyi, Email:maadeniyi@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:C2 Communicator, Email:C2-Communicator@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Venkat Bakthavachalu, Email:vbakthavachalu@vocera.com,
PIN:
Sync:Skip, VoceraID:, Name:EveryoneEverywhere_VoiceServer

Script was successfully created.
```

13. Select the users to be updated, or select Check All to automatically select all users for this update.
14. To specify that a user imported using this script is to be given access to the VMP Administrator, select the Admin Access checkbox.
15. To specify that a user imported using this script is to be given access to the VMP Web Console, select the Web Access checkbox.
16. Click Next.
17. Select Export Address Book Entries to Vocera 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 **Exporting Address Book Entries to the Vocera Voice Server** on page 34 for more information on this capability.



☑ Export Address Book Entries to Vocera

CSV File Path: C:\Users\Administrator\Desktop\addresses.csv

CSV Delimeter: , (comma)

, (comma)
; (semicolon)
TAB

Click Finish to continue.

18. 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.

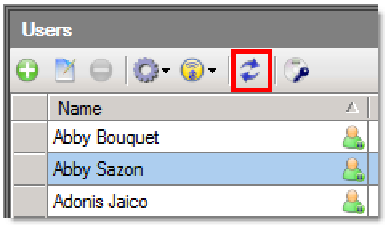
Importing Active Directory Users

A secure method of importing users to the VMP Server is through Active Directory synchronization.

The VMP Server synchronizes with the 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.

You can use automatic synchronization to synchronize VMP with Active Directory at a chosen time interval.

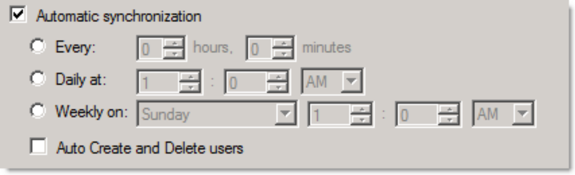
1. In the VMP Administrator, select Users & Groups > Users 👤.
2. Click the Synchronization icon ⇄ in the Users view.



Users

Name
Abby Bouquet
Abby Sazon
Adonis Jaico

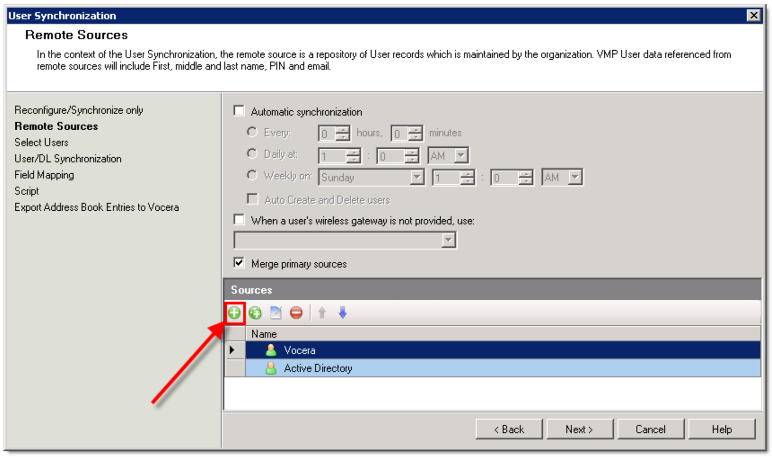
3. In the Reconfigure/Synchronize only window, select Yes, reconfigure settings.
4. Click Next.
5. Set the Automatic synchronization option to synchronize user data from the source. Select one of the following:
    - Every: Synchronize after the specified number of hours and minutes has elapsed.
    - Daily at: Synchronize every day at the specified time.
    - Weekly on: Synchronize once a week at the specified day and time.



☑ Automatic synchronization
○ Every: 0 hours, 0 minutes
○ Daily at: 1 : 0 AM
○ Weekly on: Sunday 1 : 0 AM
☐ Auto Create and Delete users

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.

6. If you have set automatic synchronization, 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.
7. Clear the wireless gateway default selector.
8. In the User Synchronization dialog, click the Add primary source with users icon ⊕ (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
Select Users
User/DL Synchronization
Field Mapping
Script
Export Address Book Entries to Vocera

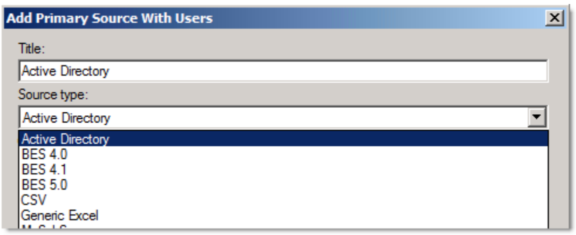
☐ Automatic synchronization
○ Every: 0 hours, 0 minutes
○ Daily at: 1 : 0 AM
○ Weekly on: Sunday 1 : 0 AM
☐ Auto Create and Delete users
☐ When a user's wireless gateway is not provided, use:
☑ Merge primary sources

Sources

Name
Vocera
Active Directory

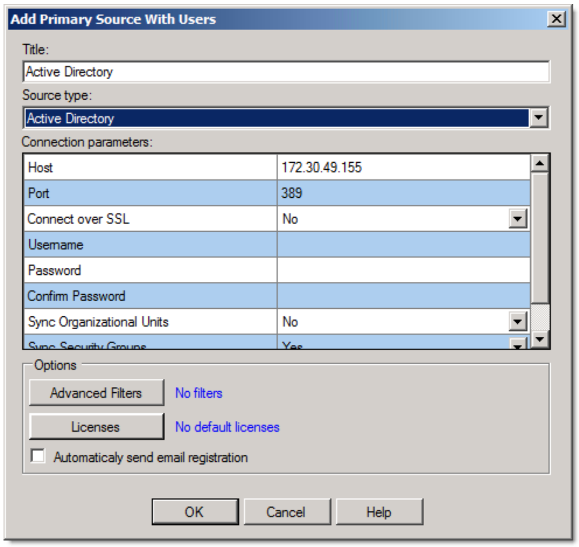
< Back | Next > | Cancel | Help

9. 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.



Title: Active Directory
Source type: Active Directory

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

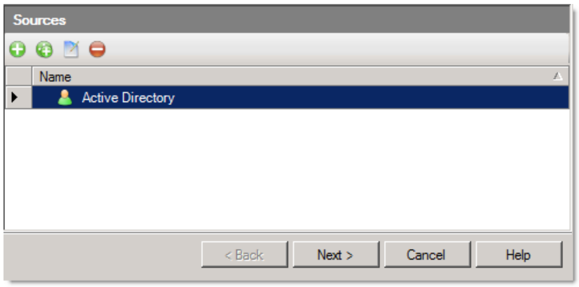


Title: Active Directory
Source type: Active Directory
Connection parameters:

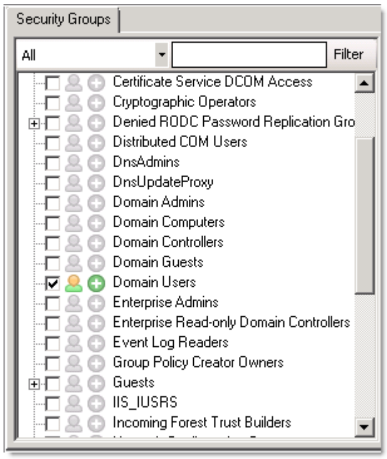
Host	172.30.49.155
Port	389
Connect over SSL	No
Username	
Password	
Confirm Password	
Sync Organizational Units	No

☐ Automaticaly send email registration

11. Configure the following options using their associated dropdown lists:
    - Sync Organization Units
    - Sync Security Groups
    - Sync Distribution Groups
12. Click OK to close the dialog.
13. The Active Directory source is configured. Make sure it is highlighted, and click Next in the User Synchronization dialog.



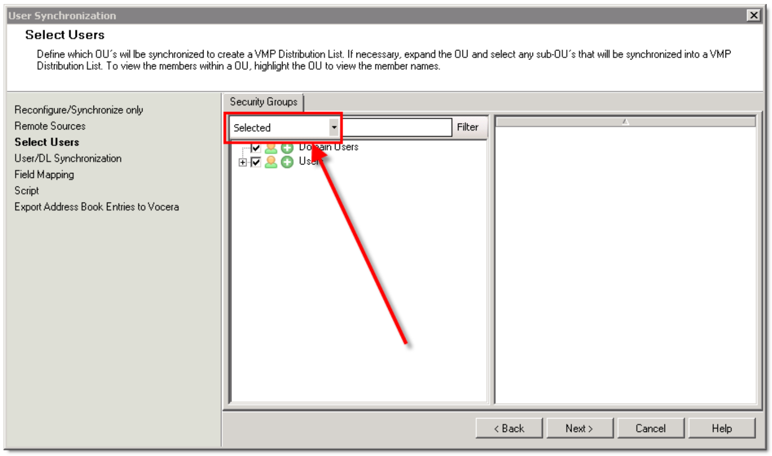
14. Select the users to import by clicking the checkbox next to the Organization Unit (OU) name. Depending on the user import configuration, the options may be included in the following three tabs:
    - Organization Units
    - Security Groups
    - Distribution Groups
15. To import an OU, select its checkbox.



☐ Certificate Service DCOM Access
☐ Cryptographic Operators
☐ Denied RODC Password Replication Gro
☐ Distributed COM Users
☐ DnsAdmins
☐ DnsUpdateProxy
☐ Domain Admins
☐ Domain Computers
☐ Domain Controllers
☐ Domain Guests
☑ Domain Users
☐ Enterprise Admins
☐ Enterprise Read-only Domain Controllers
☐ Event Log Readers
☐ Group Policy Creator Owners
☐ Guests
☐ IIS_IUSRS
☐ Incoming Forest Trust Builders

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

16. 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.



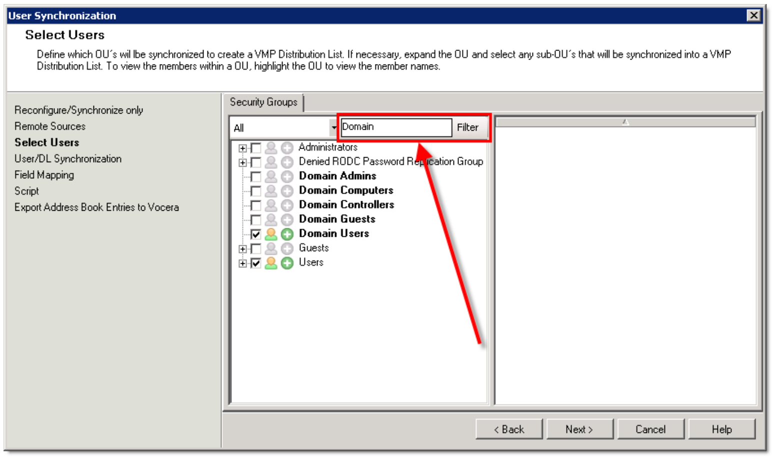
Select Users

Define which OU´s wil lbe synchronized to create a VMP Distribution List. If necessary, expand the OU and select any sub-OU´s that will be synchronized into a VMP Distribution List. To view the members within a OU, highlight the OU to view the member names.

Selected

☑ Domain Users
☑ Users

    - 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.



Select Users

Define which OU´s wil lbe synchronized to create a VMP Distribution List. If necessary, expand the OU and select any sub-OU´s that will be synchronized into a VMP Distribution List. To view the members within a OU, highlight the OU to view the member names.

All

Domain

☐ Administrators
☐ Denied RODC Password Replication Group
☐ **Domain Admins**
☐ **Domain Computers**
☐ **Domain Controllers**
☐ **Domain Guests**
☑ **Domain Users**
☐ Guests
☑ Users

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

17. Click Next.
18. In the User/DL Synchronization dialog, use the radio button selection to configure the synchronization options appropriate for your deployment. Depending on the user import configuration, the options are included in the following three tabs:
    - Organization Units

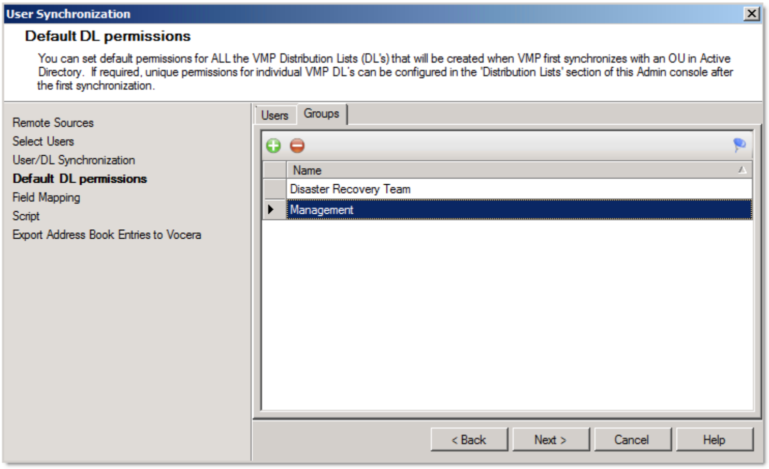
- Security Groups
- Distribution Groups

19. Click each tab to configure the options for the group.

    You can import only the users or import the existing group structures.

20. When the options are selected, click Next.

21. The Default DL Permissions dialog appears only if 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. Use the tabs to toggle between User and Group permissions. When the configuration is complete, click Next.



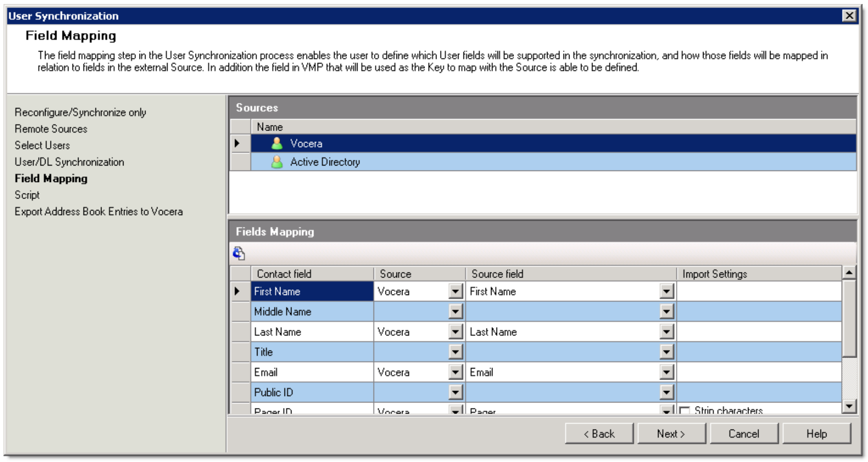
Default DL permissions

You can set default permissions for ALL the VMP Distribution Lists (DL's) that will be created when VMP first synchronizes with an OU in Active Directory. If required, unique permissions for individual VMP DL's can be configured in the 'Distribution Lists' section of this Admin console after the first synchronization.

Name
Disaster Recovery Team
Management

22. The Field Mapping dialog allows for basic field mapping from the Active Directory Source to the VMP user contact. Define the field mappings for your deployment, and click Next.

    Note: For more information about field mappings, see **Defining Contact Fields** on page 104 and **Editing Contact Fields** on page 105.



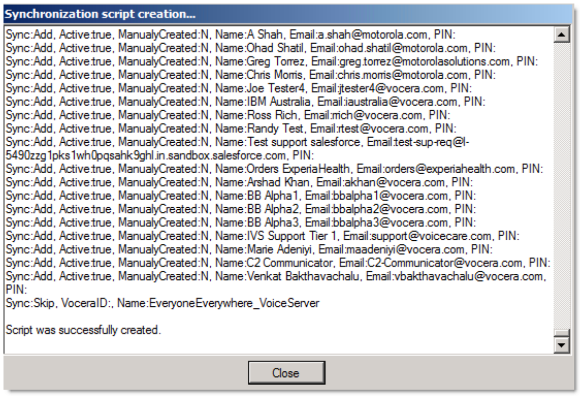
Field Mapping

The field mapping step in the User Synchronization process enables the user to define which User fields will be supported in the synchronization, and how those fields will be mapped in relation to fields in the external Source. In addition the field in VMP that will be used as the Key to map with the Source is able to be defined.

Name
Vocera
Active Directory

Contact field	Source	Source field	Import Settings
First Name	Vocera	First Name	
Middle Name			
Last Name	Vocera	Last Name	
Title			
Email	Vocera	Email	
Public ID			
Pager ID	Vocera	Pager	☐ Strip characters

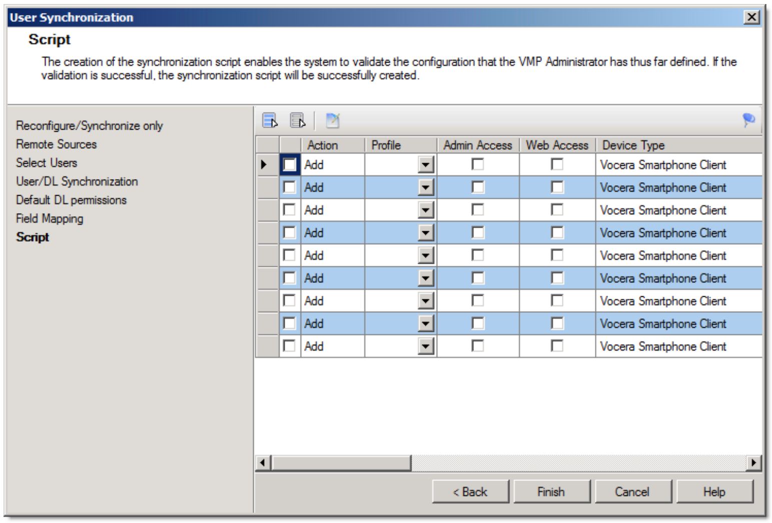
23. The synchronization script is generated by the import wizard options selected and is revealed in a script dialog box. Use the scroll bar to review the script and click Close.



```
Sync:Add, Active:true, ManualyCreated:N, Name:A Shah, Email:a.shah@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Ohad Shatil, Email:ohad.shatil@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Greg Torrez, Email:greg.torrez@motorolasolutions.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Chris Morris, Email:chris.morris@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Joe Tester4, Email:jtester4@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:IBM Australia, Email:iaustralia@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Ross Rich, Email:rrich@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Randy Test, Email:rtest@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Test support salesforce, Email:test-sup-req@l-
5490zzg1pks1wh0pqsahk9ghl.in.sandbox.salesforce.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Orders ExperiaHealth, Email:orders@experiahealth.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Arshad Khan, Email:akhan@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha1, Email:bbalpha1@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha2, Email:bbalpha2@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha3, Email:bbalpha3@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:IVS Support Tier 1, Email:support@voicecare.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Marie Adeniyi, Email:maadeniyi@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:C2 Communicator, Email:C2-Communicator@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Venkat Bakthavachalu, Email:vbakthavachalu@vocera.com,
PIN:
Sync:Skip, VoceraID:, Name:EveryoneEverywhere_VoiceServer

Script was successfully created.
```

24. The Script dialog provides the option to manually configure contact options before running the import script. This dialog is useful for defining device and wireless gateway assignments. These options can be changed manually at any time after deployment.



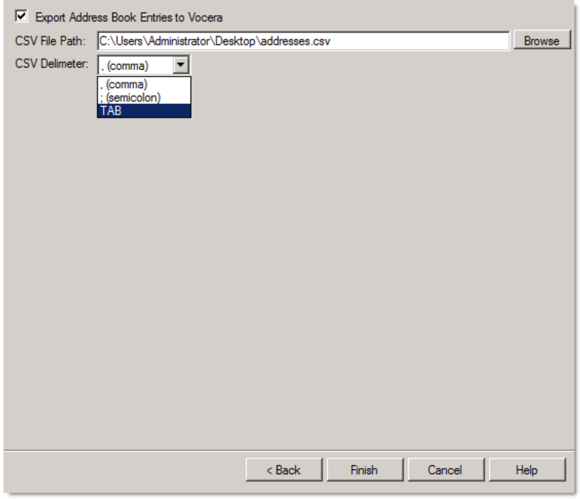
Script

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.

	Action	Profile	Admin Access	Web Access	Device Type
☐	Add		☐	☐	Vocera Smartphone Client
☐	Add		☐	☐	Vocera Smartphone Client
☐	Add		☐	☐	Vocera Smartphone Client
☐	Add		☐	☐	Vocera Smartphone Client
☐	Add		☐	☐	Vocera Smartphone Client
☐	Add		☐	☐	Vocera Smartphone Client
☐	Add		☐	☐	Vocera Smartphone Client
☐	Add		☐	☐	Vocera Smartphone Client
☐	Add		☐	☐	Vocera Smartphone Client

Click Check All to confirm the previously configured values.

25. To specify that a user imported using this script is to be given access to the VMP Administrator, select the Admin Access checkbox.
26. To specify that a user imported using this script is to be given access to the VMP Web Console, select the Web Access checkbox.
27. Click Next.
28. Select Export Address Book Entries to Vocera 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 **Exporting Address Book Entries to the Vocera Voice Server** on page 34 for more information on this capability.



☑ Export Address Book Entries to Vocera

CSV File Path: C:\Users\Administrator\Desktop\addresses.csv

CSV Delimeter: , (comma)

, (comma)
; (semicolon)
TAB

Click Finish to continue.

29. 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.

Tip: If your Active Directory server includes user photographs in the thumbnailPhoto field, you can ensure that these photographs are displayed in the Vocera Collaboration Suite. To do this, create a contact source for the Active Directory server, map the Personal Photo field to thumbnailPhoto, and set the User Key checkbox in the Email field. You must then 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 86 for more details.

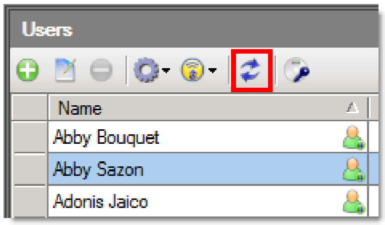
For more information on creating a contact source, see **Importing Contacts From a Source** on page 84.

Synchronizing With an Excel or CSV File

Use these steps to synchronize User or Contact sources with an Excel spreadsheet or CSV file.

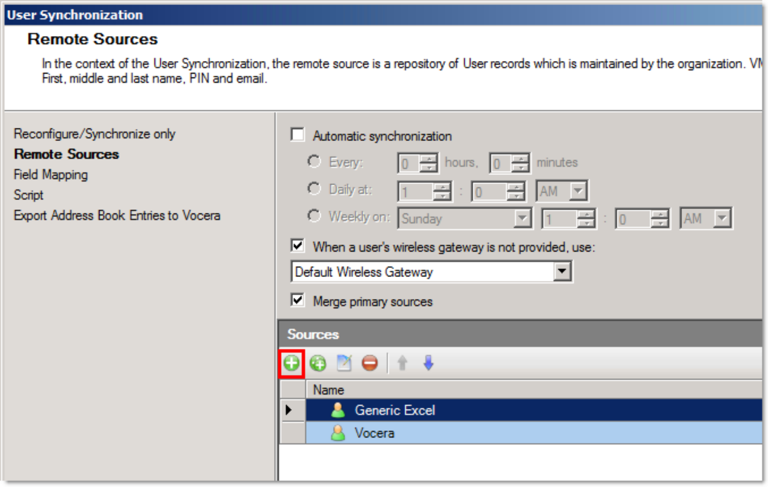
Tip: Avoid using an Excel or CSV file as a user or contact source if at all possible, as difficulties may arise if this file becomes no longer available.

1. From the VMP Administrator, select Users & Groups > Users.
2. Click the Synchronization icon in the Users view.



Abby Bouquet
Abby Sazon
Adonis Jaico

3. In the Reconfigure/Synchronize only window, select Yes, reconfigure settings. Click Next.
4. Configure the Automatic synchronization options, and clear the wireless gateway default selector.
5. Click the Add primary source with users icon (under Sources).



Remote Sources

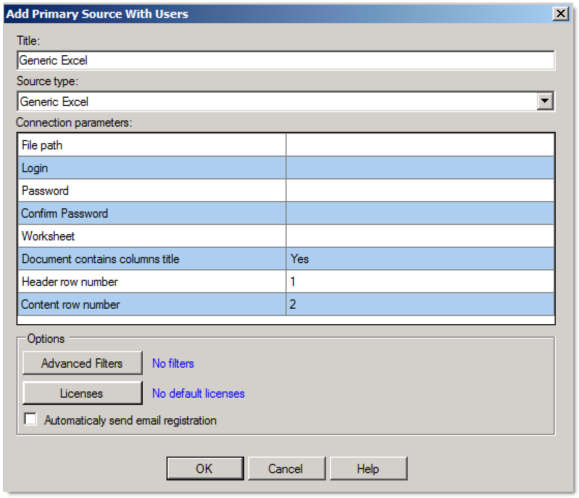
In the context of the User Synchronization, the remote source is a repository of User records which is maintained by the organization. V
First, middle and last name, PIN and email.

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
☑ When a user's wireless gateway is not provided, use: Default Wireless Gateway
☑ Merge primary sources

Generic Excel
Vocera

6. 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.
7. If your file is an Excel file, edit the connection parameters listed below and click OK.



Title: Generic Excel

Source type: Generic Excel

Connection parameters:

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

No filters

No default licenses

☐ Automaticaly send email registration

Table 11: 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.
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.

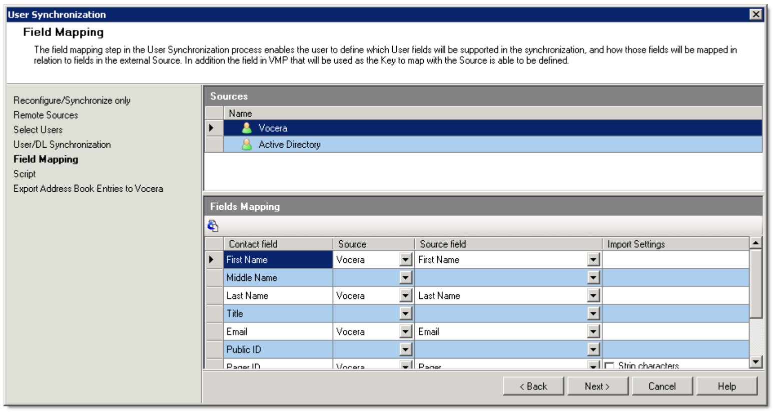
8. If your file is a CSV file, edit the connection parameters listed below and click OK.

Table 12: CSV 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 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 Automatic 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.

9. In the sources dialog, highlight the source that you have just created, and click Next.
10. The Field Mapping dialog allows for basic field mapping from the source to the VMP entry. Define the field mappings for your deployment, and click Next.

    Note: For more information about field mappings, see **Editing User Fields** on page 105 and **Defining Contact Fields** on page 104.



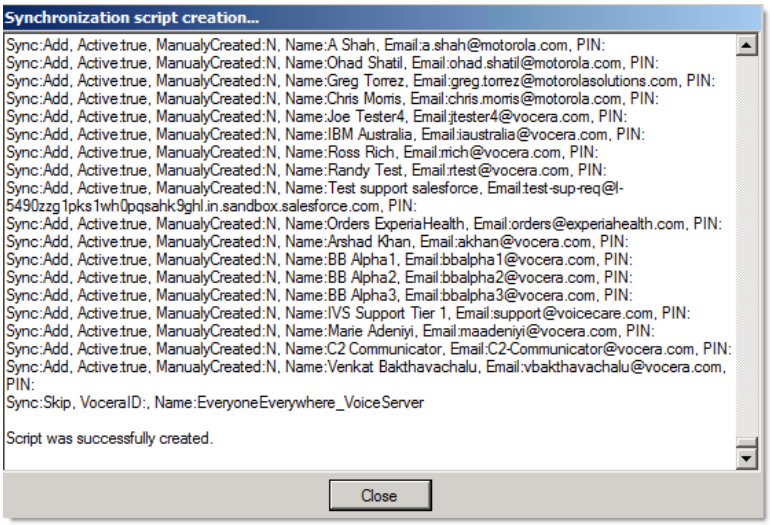
Field Mapping

The field mapping step in the User Synchronization process enables the user to define which User fields will be supported in the synchronization, and how those fields will be mapped in relation to fields in the external Source. In addition the field in VMP that will be used as the Key to map with the Source is able to be defined.

Name
Vocera
Active Directory

Contact field	Source	Source field	Import Settings
First Name	Vocera	First Name	
Middle Name			
Last Name	Vocera	Last Name	
Title			
Email	Vocera	Email	
Public ID			
Pager ID	Vocera	Pager	☐ Strip characters

11. 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.

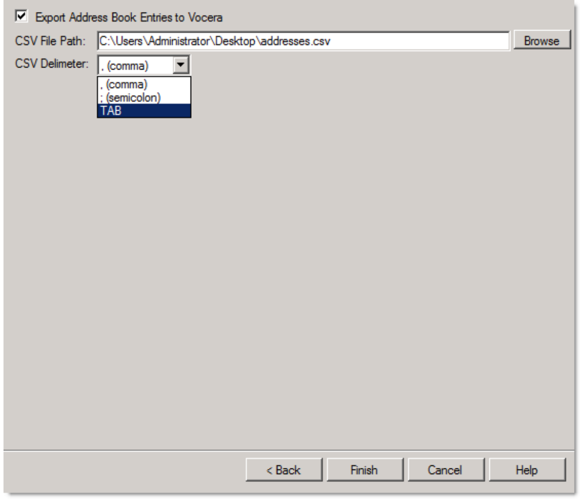


```
Sync:Add, Active:true, ManualyCreated:N, Name:A Shah, Email:a.shah@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Ohad Shatil, Email:ohad.shatil@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Greg Torrez, Email:greg.torrez@motorolasolutions.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Chris Morris, Email:chris.morris@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Joe Tester4, Email:jtester4@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:IBM Australia, Email:iaustralia@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Ross Rich, Email:rrich@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Randy Test, Email:rtest@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Test support salesforce, Email:test-sup-req@l-
5490zzg1pks1wh0pqsahk9ghl.in.sandbox.salesforce.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Orders ExperiaHealth, Email:orders@experiahealth.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Arshad Khan, Email:akhan@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha1, Email:bbalpha1@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha2, Email:bbalpha2@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha3, Email:bbalpha3@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:IVS Support Tier 1, Email:support@voicecare.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Marie Adeniyi, Email:maadeniyi@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:C2 Communicator, Email:C2-Communicator@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Venkat Bakthavachalu, Email:vbakthavachalu@vocera.com,
PIN:
Sync:Skip, VoceraID:, Name:EveryoneEverywhere_VoiceServer

Script was successfully created.
```

The Script dialog provides the option to manually configure contact options before running the import script. This dialog is useful for defining device and wireless gateway assignments. These options can be changed manually at any time after deployment.

12. Click Check All to confirm the previously configured values.
13. To specify that a user imported using this script is to be given access to the VMP Administrator, select the Admin Access checkbox.
14. To specify that a user imported using this script is to be given access to the VMP Web Console, select the Web Access checkbox.
15. Click Next.
16. Select Export Address Book Entries to Vocera 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 **Exporting Address Book Entries to the Vocera Voice Server** on page 34 for more information on this capability.



☑ Export Address Book Entries to Vocera

CSV File Path: C:\Users\Administrator\Desktop\addresses.csv

CSV Delimeter: , (comma)

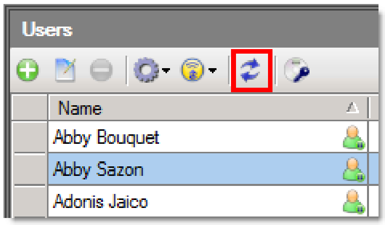
Click Finish to continue.

17. 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 With SQL

Use these steps to synchronize User or Contact sources with an SQL database.

1. From the VMP Administrator, select Users & Groups > Users.
2. Click the Synchronization icon in the Users view.

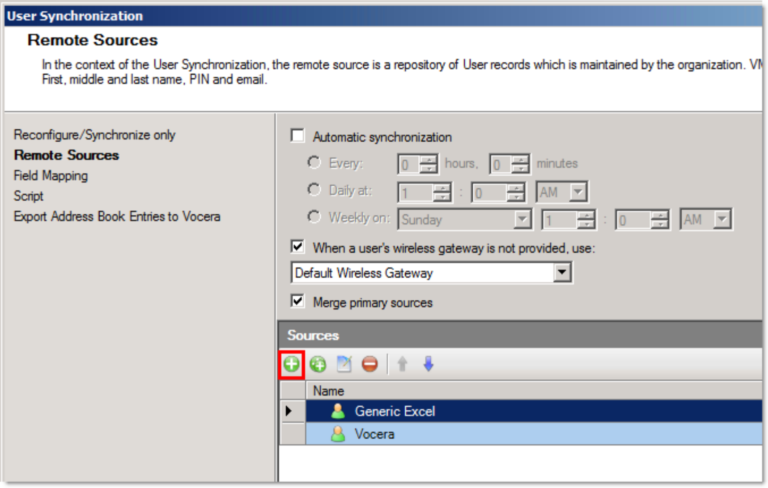


Abby Bouquet

Abby Sazon

Adonis Jaico

3. In the Reconfigure/Synchronize only window, select Yes, reconfigure settings. Click Next.
4. In the User Synchronization dialog, click the Add primary source with users icon (under Sources).



In the context of the User Synchronization, the remote source is a repository of User records which is maintained by the organization. VI
First, middle and last name, PIN and email.

☐ Automatic synchronization

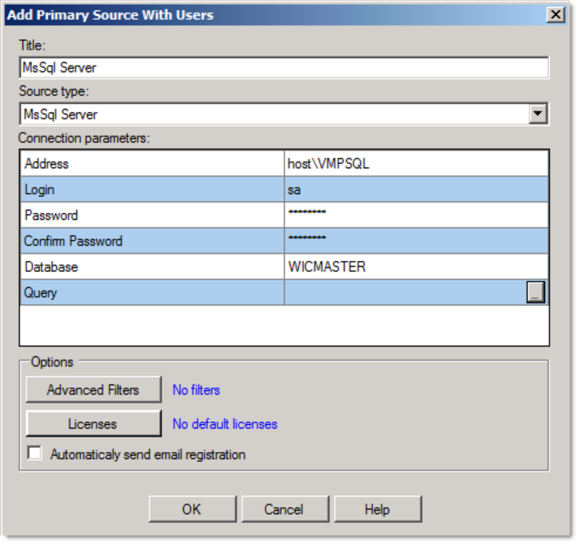
☑ When a user's wireless gateway is not provided, use:

Default Wireless Gateway

☑ Merge primary sources

Name
Generic Excel
Vocera

5. Configure the Automatic synchronization options, and click to clear the wireless gateway default selector.
6. 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.
7. Enter the Connection Parameters and click OK.



Title: MsSql Server

Source type: MsSql Server

Connection parameters:

Address	host\VMPSQL
Login	sa
Password	********
Confirm Password	********
Database	WICMASTER
Query	

No filters

No default licenses

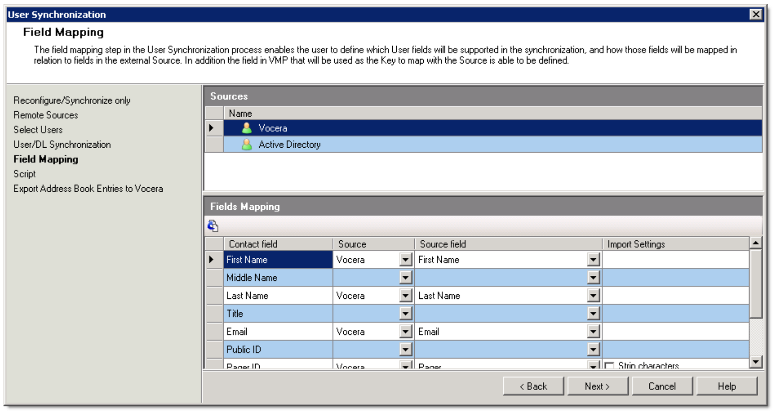
☐ Automaticaly send email registration

Table 13: 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 specifc query options for the import.

8. In the sources dialog, highlight the SQL source that you have just created, and click Next.
9. The Field Mapping dialog allows for basic field mapping from the source to the VMP entry. Define the field mappings for your deployment, and click Next.

Note: For more information about field mappings, see **Editing User Fields** on page 105 and **Defining Contact Fields** on page 104.



Field Mapping

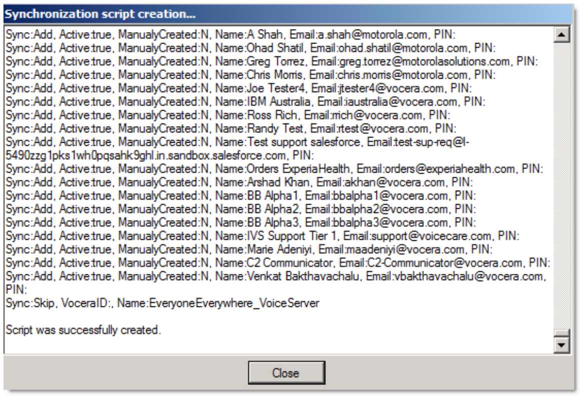
The field mapping step in the User Synchronization process enables the user to define which User fields will be supported in the synchronization, and how those fields will be mapped in relation to fields in the external Source. In addition the field in VMP that will be used as the Key to map with the Source is able to be defined.

Name
Vocera
Active Directory

Fields Mapping

Contact field	Source	Source field	Import Settings
First Name	Vocera	First Name	
Middle Name			
Last Name	Vocera	Last Name	
Title			
Email	Vocera	Email	
Public ID			
Pager ID	Vocera	Pager	☐ Strip characters

10. 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.

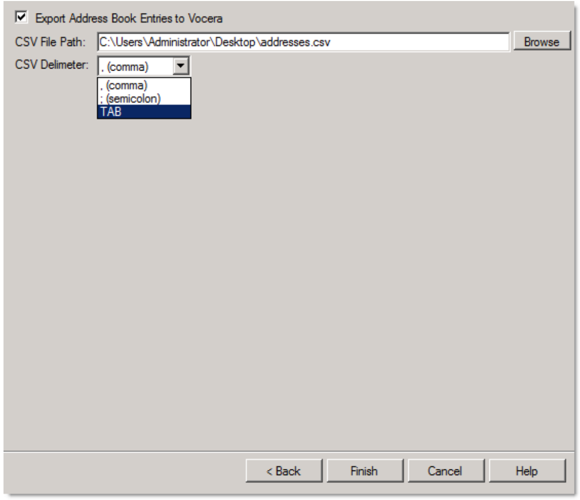


```
Sync:Add, Active:true, ManualyCreated:N, Name:A Shah, Email:a.shah@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Ohad Shatil, Email:ohad.shatil@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Greg Torrez, Email:greg.torrez@motorolasolutions.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Chris Morris, Email:chris.morris@motorola.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Joe Tester4, Email:jtester4@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:IBM Australia, Email:iaustralia@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Ross Rich, Email:rrich@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Randy Test, Email:rtest@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Test support salesforce, Email:test-sup-req@l-
5490zzg1pks1wh0pqsahk9ghl.in.sandbox.salesforce.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Orders ExperiaHealth, Email:orders@experiahealth.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Arshad Khan, Email:akhan@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha1, Email:bbalpha1@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha2, Email:bbalpha2@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:BB Alpha3, Email:bbalpha3@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:IVS Support Tier 1, Email:support@voicecare.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Marie Adeniyi, Email:maadeniyi@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:C2 Communicator, Email:C2-Communicator@vocera.com, PIN:
Sync:Add, Active:true, ManualyCreated:N, Name:Venkat Bakthavachalu, Email:vbakthavachalu@vocera.com,
PIN:
Sync:Skip, VoceraID:, Name:EveryoneEverywhere_VoiceServer

Script was successfully created.
```

The Script dialog provides the option to manually configure contact options before running the import script. This dialog is useful for defining device and wireless gateway assignments. These options can be changed manually at any time after deployment.

11. Click Check All to confirm the previously configured values.
12. To specify that a user imported using this script is to be given access to the VMP Administrator, select the Admin Access checkbox.
13. To specify that a user imported using this script is to be given access to the VMP Web Console, select the Web Access checkbox.
14. Click Next.
15. Select Export Address Book Entries to Vocera 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 **Exporting Address Book Entries to the Vocera Voice Server** on page 34 for more information on this capability.



☑ Export Address Book Entries to Vocera

CSV File Path: C:\Users\Administrator\Desktop\addresses.csv

CSV Delimeter: , (comma)

, (comma)
; (semicolon)
TAB

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.

Adding and Deleting Users Manually

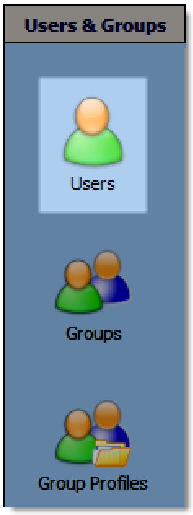
If you want to add a user that is not included in your remote resource, you can add the user manually. You can also manually delete users from the system.

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.
3. Enter the following end-user settings.

Table 14: 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 26 for more information on integrating with the Vocera Voice Server.
Profile	Select from this dropdown list to associate the user with a group profile. See **Group Profiles** on page 82 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 AD Account 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 Vocera Server 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.
5. To enable mobile device access, select the Enable checkbox, and select the device type from the Device type dropdown list.
6. 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 57.

7. 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.
9. Click Finish to finish creating the new user.

Deleting a User

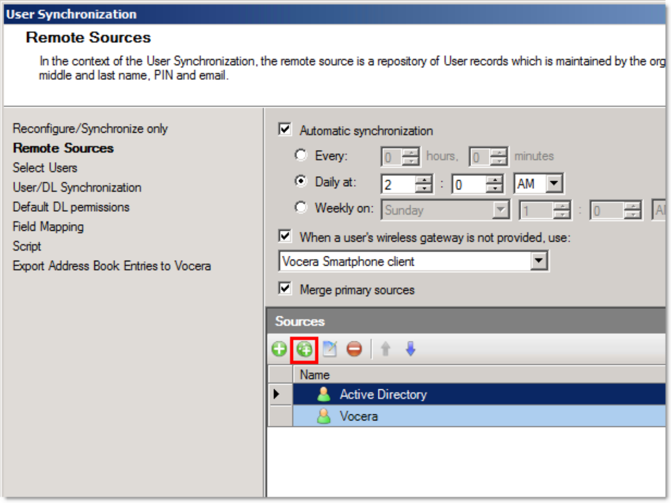
You can manually delete any user, and can optionally wipe all data stored in the user's smartphone application.

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.

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

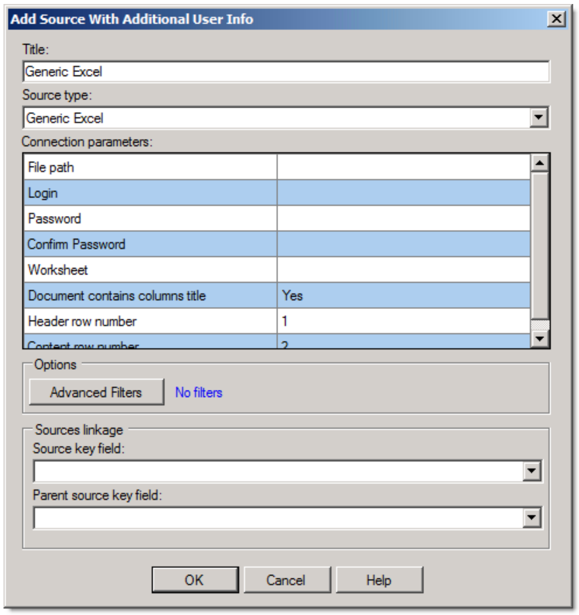
In the context of the User Synchronization, the remote source is a repository of User records which is maintained by the org
middle and last name, PIN and email.

☑ Automatic synchronization
○ Every: 0 hours, 0 minutes
● Daily at: 2 : 0 AM
○ Weekly on: Sunday 1 : 0

☑ When a user's wireless gateway is not provided, use:
Vocera Smartphone client

☑ Merge primary sources

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.



Title: Generic Excel

Source type: Generic Excel

Connection parameters:

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

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 Active Directory Users** on page 39
- Vocera Server: see **Vocera Voice Server Integration** on page 26
- Excel and CSV files: see **Synchronizing With an Excel or CSV File** on page 45
- SQL: see **Synchronizing With SQL** on page 48

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.

Monitoring Email 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 57.

Configuring VMP for Message Email Integration

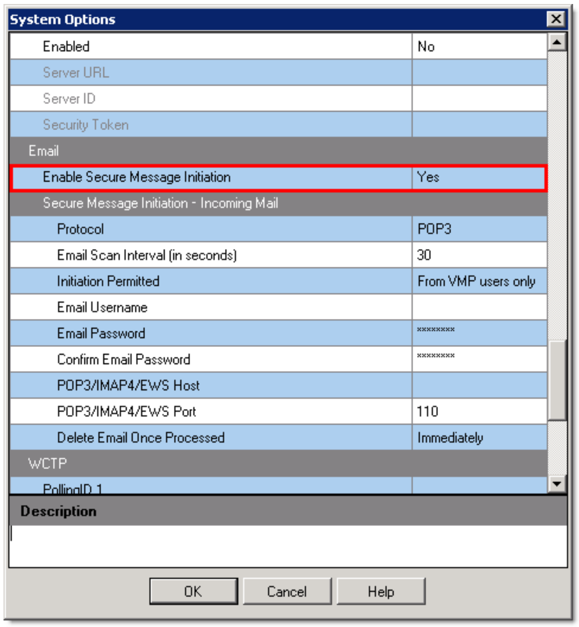
Use the following steps to configure VMP to send messages using email.

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 and select:

Configuration > System Options

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



Enabled	No
Server URL	
Server ID	
Security Token	
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	

4. In the Secure Message Initiation - Incoming Mail section, configure the following settings as appropriate for your deployment:

Table 15: Email configuration options

Setting	Description
Protocol	Use the dropdown list to select from the following options: • POP3 • IMAP4 • Exchange Web Services
Email Scan Interval	How often the mailbox is to be polled for messages. This is measured in seconds. The default is 30 seconds.
Initiation Permitted	Who can initiate messages by email. This is one of the following: • 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.
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).
Delete Email Once Processed	How often theVMP Server will remove emails from the monitored mailbox. This is one of the following: • Immediately: The VMP Server deletes the email immediately after it has been converted to a message. • Once/Day: The VMP Server deletes all processed emails that are older than 24 hours. • Never: The VMP Server never deletes any email. Select this setting only if email is deleted by another process or person.

5. Scroll back to System and Networking > Email.
6. Set Enable Outgoing Email to Yes. This ensures that delivery and response updates can be sent back to the email initiator.
7. Configure the following settings:

Table 16: Outgoing email configuration options

Setting	Description
Display Name	The name to use when sending email.
Email Address	The email address from which email is to be sent.
SMTP Server	The SMTP server to use for outgoing email.
SMTP Port	The port to use for outgoing email.
SMTP Authentication	Whether to use SMTP authentication. If this is set to Yes, additional fields appear in which you must enter the email username, email password, and a confirmation of the email password.

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:

Table 17: Supported XML tags

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.
To:	A list of one or more recipient email addresses.
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 From: tag.
ResponseType:	The response type associated with the message. This is one of the following: • None: No response is required. • Multi: Recipients must select from one or more responses defined in the message.
Responses:	When ResponseType is set to Multi, this is a container tag for the responses defined for the message. Each response is contained in an EmailPagingAlertResponse, which is defined below.

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

Table 18: EmailPagingAlertResponse 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>
```

Configuring User Devices and Client Applications

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.

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. From the VMP Administrator, 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.

Setting Up 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 IP address of the VMP Server. You can autoconfigure the Vocera Collaboration Suite client to display the 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. When the Vocera Collaboration Suite client is started, it searches for this entry and displays the VMP Server's IP address if the entry is found.

Note: In a clustered VMP Server environment, set autodiscovervs to be the IP address of the load balancer.

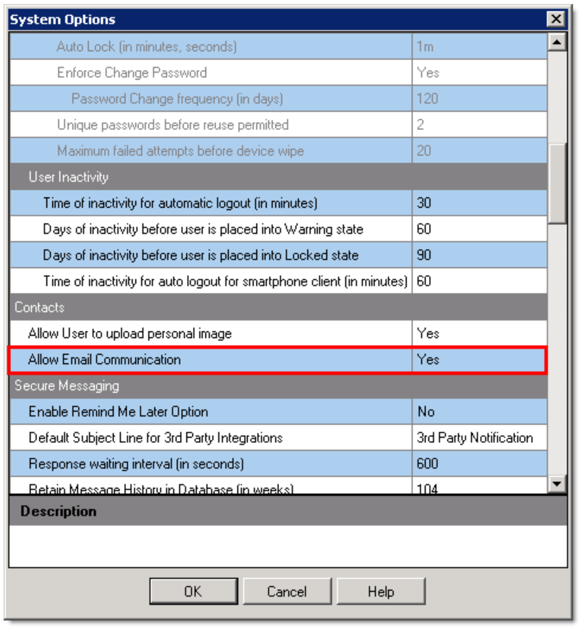
Enabling Email Communication

Use these steps to 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

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.



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
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

4. Click OK to save your change.

Configuring the VMP Server For Secure Connections

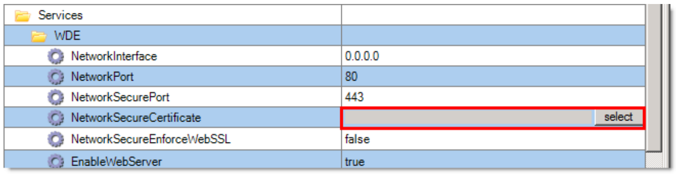
If the VMP Server was not configured to use SSL during installation, you can use the VMP Enterprise Manager to configure it to use SSL after installation.

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. From the left pane, select Configuration .

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.

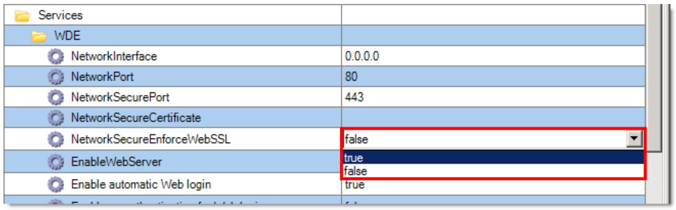


Services	
WDE	
NetworkInterface	0.0.0.0
NetworkPort	80
NetworkSecurePort	443
NetworkSecureCertificate	select
NetworkSecureEnforceWebSSL	false
EnableWebServer	true

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 false
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 59.

7. Click Save to save your changes. In the confirmation dialog box that appears, click OK.
8. 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

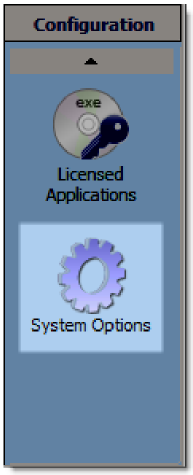
From the VMP Administrator, you can enforce that all communications between the VMP Server and VMP clients are to use SSL. This ensures that all communications are securely encrypted.

Note: The use of SSL can be enforced during the installation of the VMP Server. See **Installing the VMP Server** on page 10 for details.

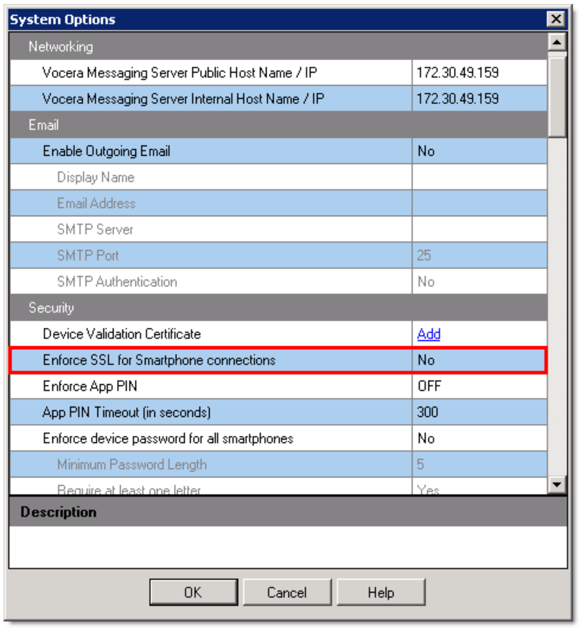
If you are updating a previously installed VMP Server to enforce the use of SSL, all existing VMP clients that are not using SSL must re-register to use the VMP Server, as the connection protocol used by a client is specified when the client is registered.

Before you can enforce SSL use, you must configure a SSL certificate. For details, see **Configuring the VMP Server For Secure Connections** on page 58.

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



3. 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.



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

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

VMP Security and Encryption Structure

All transmissions between the VMP Server and client applications on iOS and Android devices employ secure communication methods. The method employed depends on the device's operating system and on the environment in which it is being used.

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.

Using Comet Notifications

When a Vocera Collaboration Suite client on the iOS or Android operating system is operating within the organization's Wi-Fi network, and a message needs to be sent from the VMP Server to the device, the server uses Comet to send a content-less notification to the device.

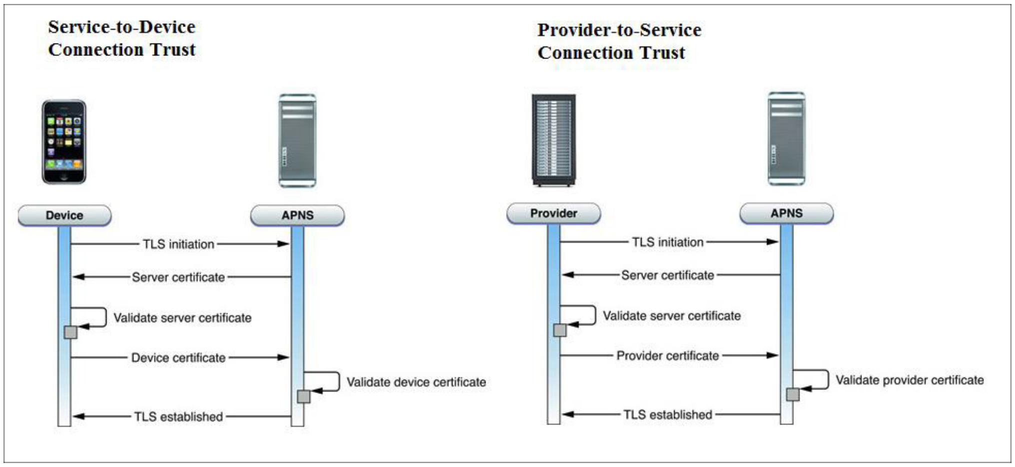
When the device receives the notification, it uses its normal connection to the VMP Server to retrieve the message. This connection is secure if it has been configured to use SSL.

In the VMP Enterprise Manager, you can configure the VMP Server to force the use of SSL when communicating with client applications. See **Enforcing SSL on the VMP Server** on page 59 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.


Service-to-Device Connection Trust
Device
APNS
TLS initiation
Server certificate
Validate server certificate
Device certificate
Validate device certificate
TLS established
Provider-to-Service Connection Trust
Provider
APNS
TLS initiation
Server certificate
Validate server certificate
Provider certificate
Validate provider certificate
TLS established

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.

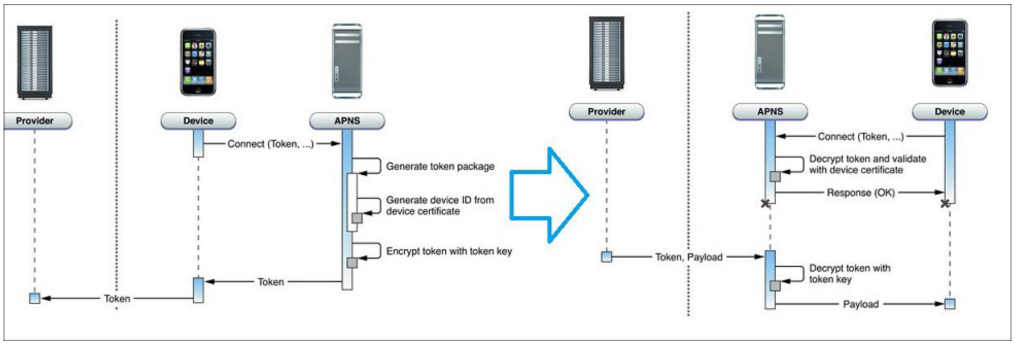
APNS includes a default Quality of Service (QoS) component that performs a store-and-forward function. If APNS attempts to deliver a message when the device is offline, the QoS stores the notification. It retains only one notification per application on a device: the last notification received from a 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.

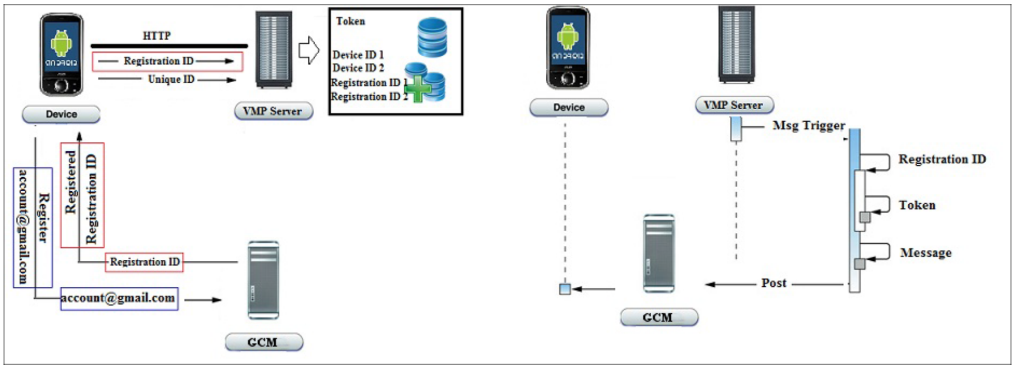
The diagram below shows the token relationship between the VMP Server, APNS, and the client device.


Provider
Device
APNS
Connect (Token, ...)
Generate token package
Generate device ID from device certificate
Encrypt token with token key
Token
Token
Provider
APNS
Device
Connect (Token, ...)
Decrypt token and validate with device certificate
Response (OK)
Token, Payload
Decrypt token with token key
Payload

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

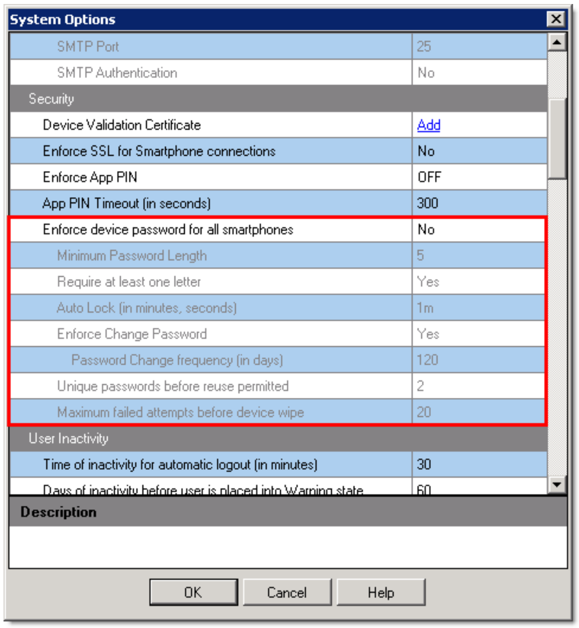
The Android-based Vocera Collaboration Suite application must register with the VMP Server to receive push notifications. It does this right after it is installed on a device.

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.

Password Enforcement

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.



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
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

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.
4. Scroll to Security > Enable device password for all smartphones, and select Yes.
5. Configure the following options:

Table 19: 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 *N* most recent passwords used, where *N* 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.

Vocera Messaging Platform Failover

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 fails. 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 **Installing a VMP Cluster** on page 16.

Tip: Configure email alert notifications to receive an alert when a failover occurs. For details, see **Configuring Failover Email Notifications** on page 66.

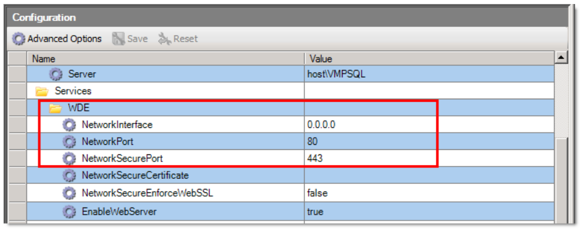
Configuring Vocera Messaging Platform Failover

Use these steps to create a DNS round robin clustered VMP Server with a secondary IP address associated with the main server hostname.

A Load Balancer is used to redirect traffic to the node of the cluster that is currently active. The DNS entry or IP address of the Load Balancer serves as the point of contact for the outside world. If the primary VMP Server fails, the Load Balancer redirects traffic from the primary server to the secondary server.

In the event of a failover, the VMP services must be manually re-started for the application to function. The data exchange service is restarted on the secondary node.

1. Add the IP address for each node as the VMP hostname on the DNS server.
2. If your network is using non-standard ports, configure the network port information.
    a. Start the VMP Enterprise Manager, and select Configuration ⚙.
    b. Enter the network port information.



Name	Value
Server	host\VMPSQL
Services	
WDE	
NetworkInterface	0.0.0.0
NetworkPort	80
NetworkSecurePort	443
NetworkSecureCertificate	
NetworkSecureEnforceWebSSL	false
EnableWebServer	true

c. Click Save. When prompted, click OK to restart the Vocera Data Exchange Service.

If DNS fails over to the secondary node, the required VMP services must be restarted. The secondary failover should also be pre-configured to point to the correct SQL database. For details about post-failover tasks, see **Post Failover Configuration** on page 67.

Failover Configuration Scenarios

This is a list of VMP Server failover configuration scenarios.

Table 20: Failover configuration scenarios

Node	Description
Primary Vocera Messaging Platform (VMP Server 1)	• 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)	• 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. 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.
The Load Balancer in conjunction with the VMP Server pair	• 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	• 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.

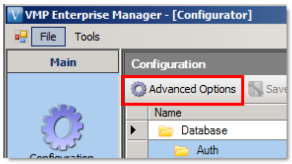
Configuring Failover Email Notifications

Use these steps to configure failover email notifications.

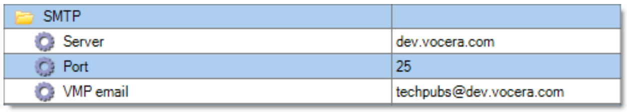
1. From the VMP Server, start the VMP Enterprise Manager:

   Start > All Programs > VMP > VMP Enterprise Manager

2. Select Configuration > Advanced Options ⚙.

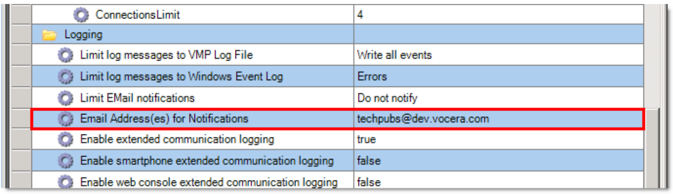


3. In the SMTP section, type the SMTP mail settings for your deployment.



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

4. 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 VMP Server configuration scenario is changed.

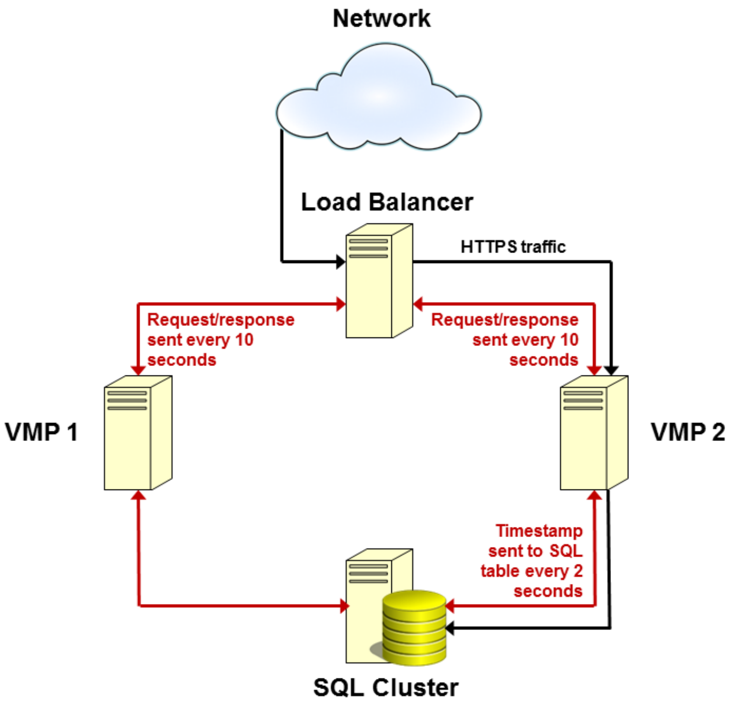
Primary VMP Server - VMP Server 1

- 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.


Network
Load Balancer
HTTPS traffic
Request/response sent every 10 seconds
Request/response sent every 10 seconds
VMP 1
VMP 2
Timestamp sent to SQL table every 2 seconds
SQL Cluster

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).

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

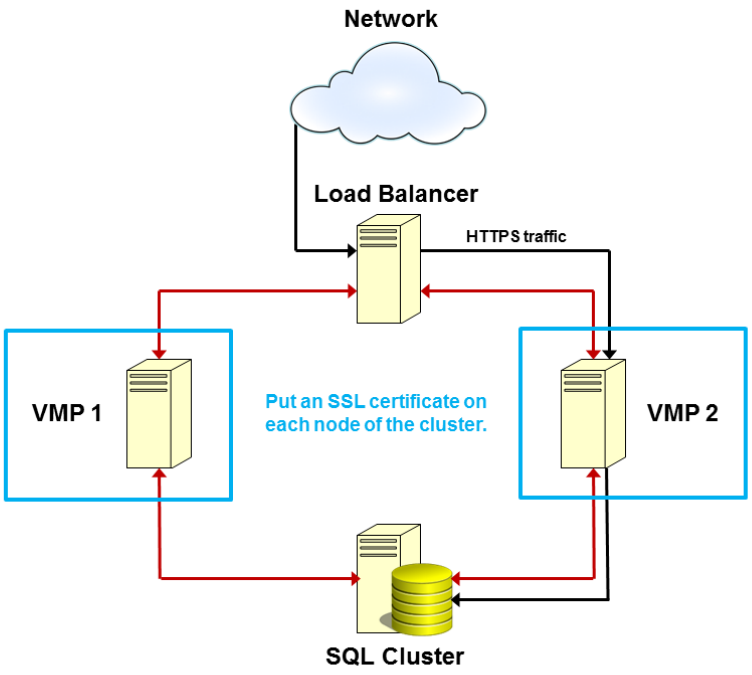
To reconfigure VMP Server 1 to be the primary server, follow the steps shown here.

1. The Administrator must shut down the Vocera Data Exchange Windows service on VMP Server 2.
2. The Administrator must restart the Vocera Data Exchange Windows service on VMP Server 1. VMP Server 1 will assume primary server status.
3. The Administrator must 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 further action is required.

Using 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

SQL AlwaysOn Availability Groups is a high availability and disaster recovery solution that provides an enterprise-level alternative to database mirroring in SQL Server 2012 environments.

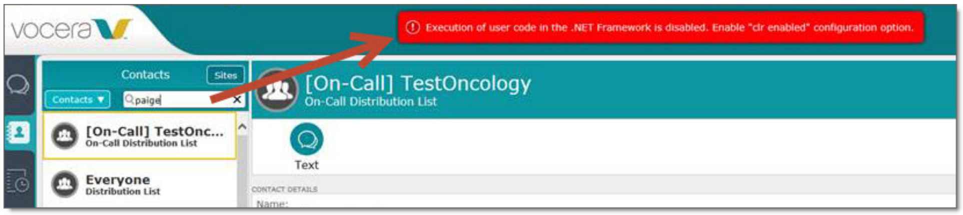
An AlwaysOn Availability Group supports a failover environment for a discrete set of user databases, known as availability databases, that fail over together. The availability group supports a set of read-write primary databases and one to four sets of corresponding secondary databases.

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:


Execution of user code in the .NET Framework is disabled. Enable "clr enabled" configuration option.

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.

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

Use these steps to perform a remote wipe from the VMP Administrator.

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 a Remote Wipe Using Microsoft Exchange

Use these steps to perform a remote wipe using Microsoft Exchange.

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

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 a Remote Wipe Using Outlook Web

Use these steps to perform a remote wipe using Outlook Web.

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 a Remote Wipe Using a Mobile Device Management Solution

Use these steps to perform a remote wipe using a Mobile Device Management (MDM) solution.

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

Use these steps to perform a 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`

Updating the APNS Certificate

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 Apple Push Notification Service (APNS), which then sends the notification to the device.

The connection to the APNS uses a security certificate, which is included as part of the VMP Server installation process. This certificate needs to be updated every year. The Vocera support team will contact you when your APNS certificate is about to expire.

After you have received your updated certificate file, you can use the VMP Enterprise Manager to update the VMP Server to use the new certificate.

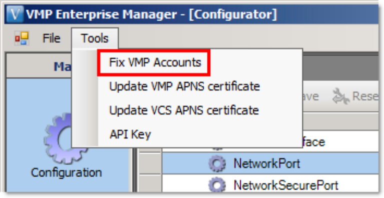
1. Start the VMP Enterprise Manager.
2. From the Tools menu, select Update VCS APNS certificate to update the APNS certificate for the Vocera Collaboration Suite client.
3. Specify the location of the certificate file that has been provided to you, and click OK.

The APNS certificate is now updated.

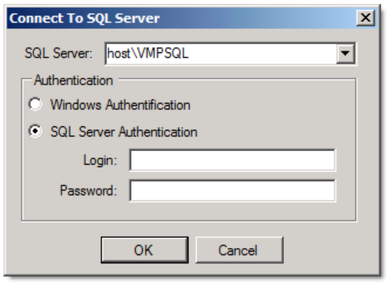
Changing the SQL Accounts for the VMP Server

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.


VMP Enterprise Manager - [Configurator]
File
Tools
Fix VMP Accounts
Update VMP APNS certificate
Update VCS APNS certificate
API Key
Ma
ave
Rese
face
NetworkPort
NetworkSecurePort
Configuration

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

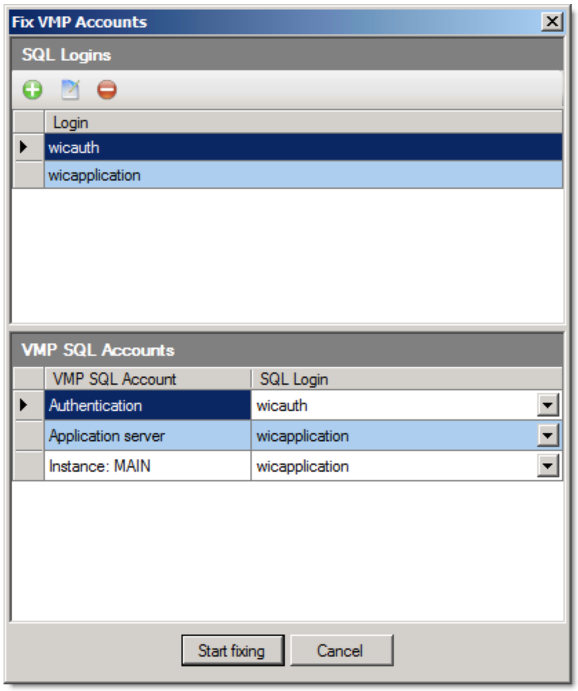


SQL Server: host\VMPSQL

○ Windows Authentification

● SQL Server Authentication

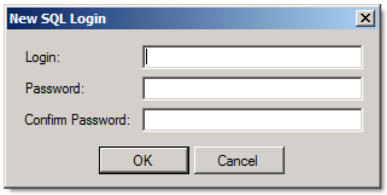
   a. Select the authentication method to use by selecting either Windows Authentication or SQL Server Authentication.
   b. If you have selected SQL Server Authentication, enter your SQL login and password in the Login and Password fields.
   c. Click OK. The Fix VMP Accounts window appears.



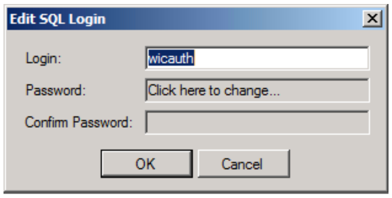
Login
wicauth
wicapplication

VMP SQL Account	SQL Login
Authentication	wicauth
Application server	wicapplication
Instance: MAIN	wicapplication

4. To add a new SQL account:
   a. Click Add . The New SQL Login dialog appears.



   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 Edit SQL Login dialog appears.



Login: wicauth

Password: Click here to change...

Confirm Password:

   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. 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.

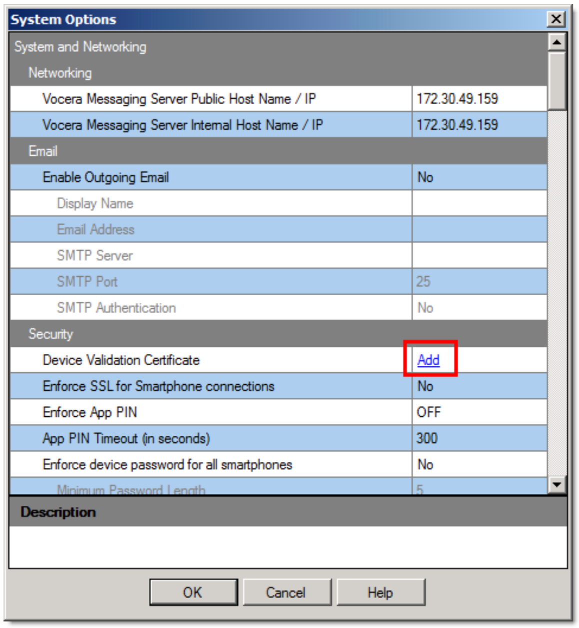
Uploading a Device Certificate

If you are using a Mobile Device Management solution to install a device certificate on your devices, you can upload this 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 device certificate to the VMP Server:

1. Start the VMP Administrator and select:

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



System and Networking	
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

4. Locate the certificate on your computer, and click Open. The device certificate is now uploaded.

The VMP Administrator

Learn about using the VMP Administrator.

VMP Administrator Overview

The VMP Administrator is an application that enables you to configure the VMP Server and create users and groups.

The VMP Administrator can be installed on the same computer as the VMP Server or on a separate machine. Use the VMP Administrator to:

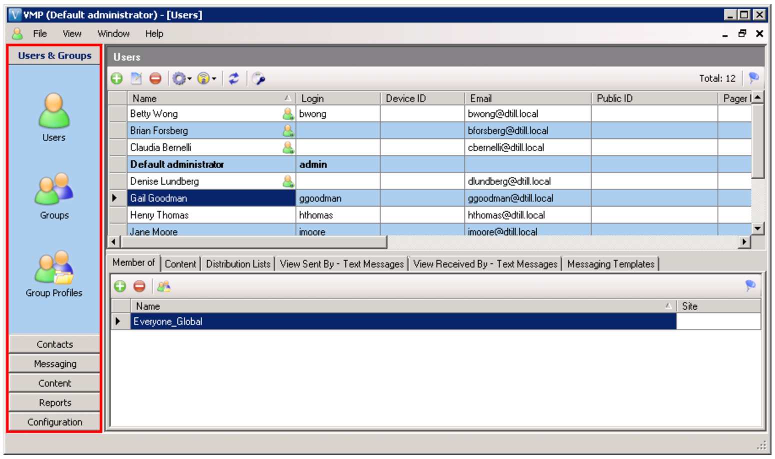
- Configure users to receive messages
- Create and manage users and access groups
- Create and manage Distribution Lists and On-Call Distribution Lists
- Create and manage Messaging Templates
- Send messages, create response options, and view the status of messages

The console includes the following modules:

Table 21: VMP Administrator modules

Module	Description
Users & Groups	Import, configure, and manage users.
Contacts	Create and manage contacts, groups, and Contacts Distribution Lists.
Messaging	Configure notification settings, create Messaging templates, and create and manage Distribution Lists.
Content	Add media assets to the VMP Server for use from the client.
Reports	Generate view incidents and logs, and create and send reports.
Configuration	Configure wireless gateways, contact fields and source mapping, synchronization, and configure plugins.

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



Name	Login	Device ID	Email	Public ID	Pager I
Betty Wong	bwong		bwong@dtill.local		
Brian Forsberg			bforsberg@dtill.local		
Claudia Bernelli			cbernelli@dtill.local		
Default administrator	**admin**				
Denise Lundberg			dlundberg@dtill.local		
Gail Goodman	ggoodman		ggoodman@dtill.local		
Henry Thomas	hthomas		hthomas@dtill.local		
Jane Moore	imoore		imoore@dtill.local		

Name	Site
Everyone_Global	

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.

Standalone VMP Administrator Requirements

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.

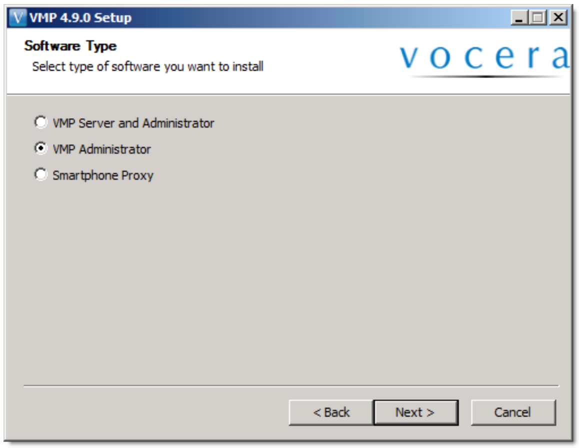
To use the VMP Administrator on a standalone server, you must have the following:

- 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 Server

Use these steps to install the VMP Administrator on a standalone server.

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



Software Type

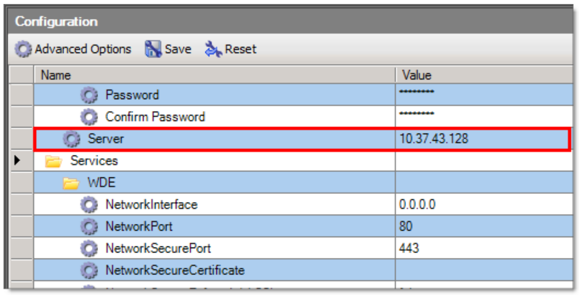
Select type of software you want to install

○ VMP Server and Administrator

● VMP Administrator

○ Smartphone Proxy

4. Accept the default Destination Folder, or click Browse to select a custom installation folder, then click Install.
5. In the VMP Enterprise Manager Configuration window, click in the Server row's Value column, and enter the IP address for the SQL server.



Name	Value
Password	********
Confirm Password	********
Server	10.37.43.128
Services	
WDE	
NetworkInterface	0.0.0.0
NetworkPort	80
NetworkSecurePort	443
NetworkSecureCertificate	

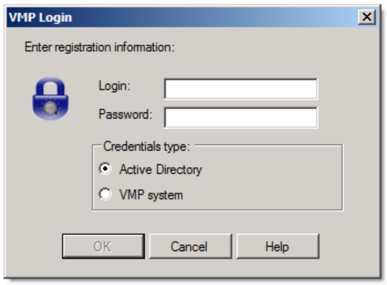
6. In the Active Directory Server row, click in the Value column and enter the IP address for the Active Directory server.
7. Click Save and close the VMP Enterprise Manager.
8. Click Finish.

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.



Note: The Credentials type radio buttons appear only if the VMP Server has been configured to allow logging in using Active Directory credentials. See **Configuring VMP for Active Directory** on page 34 for more information.

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 51 for details on setting the Enable PC Admin Console Access option to authorize user access to the VMP Administrator.

4. Enter 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 10 for more details.

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

Users and Groups

The Users & Groups module provides features to import, create, and manage platform users.

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

Use groups to create user sets and Distribution Lists to manage access permissions and on-call scheduling.

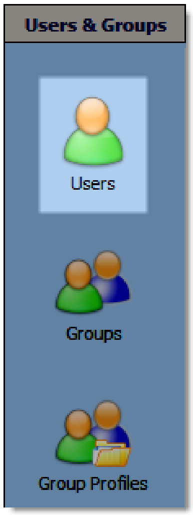
Note: Some of the features found in the Users & Groups module are covered in **Deploying VMP** on page 21:

- **Importing and Synchronizing Users and Contacts** on page 35, which includes synchronization with Active Directory, and importing from Excel, CSV files, SQL, or Vocera Server
- **Sending Installation Information to User Devices** on page 57

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 end-user settings as needed. For more information on the fields in the End-User Settings pane, see **Adding and Deleting Users Manually** on page 51.
5. Click Next. The Push Technology and Licensing window appears.
6. To enable or disable mobile device access, select or clear the Enable checkbox. If Enable is selected, you can change the device type by selecting from the Device type dropdown list, or change the registration information by entering new text in the fields provided.
7. 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.

Note: If you select Enforce PIN, this user 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.

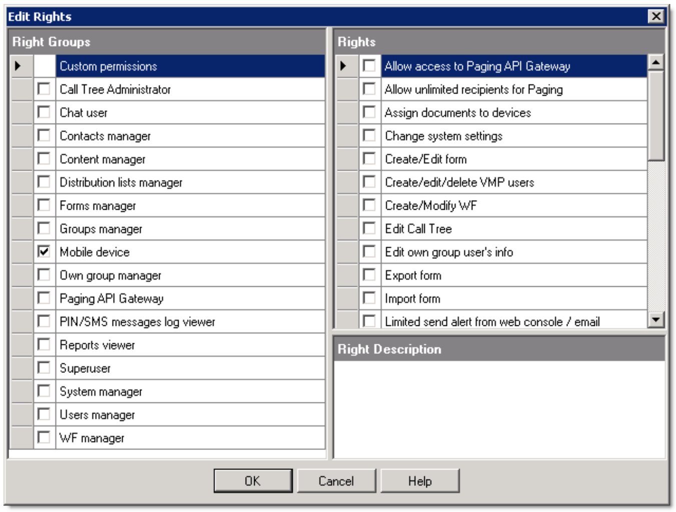
8. In the VMP Applications On Device pane, to grant or deny access to a VMP application, select or clear the checkbox next to the application name.
9. Click Finish to finish editing the user information.

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.
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.

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.

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.
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.

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:

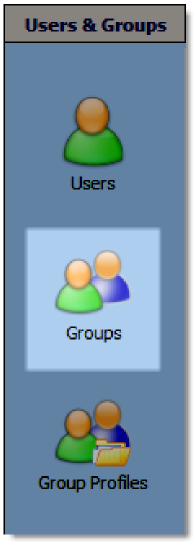
- Create, rename, and delete groups
- Add users to a group and remove users from a group
- Indicate what items are to be made accessible to the group

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

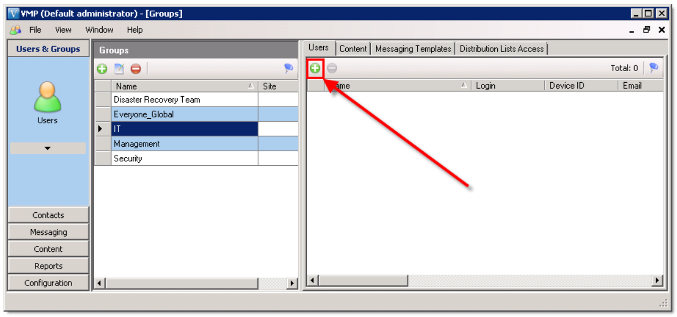
From the Users & Groups module, you can delete any existing group.

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.



Name	Site
Disaster Recovery Team	
Everyone_Global	
IT	
Management	
Security	

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

Note: 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.

Note: 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.

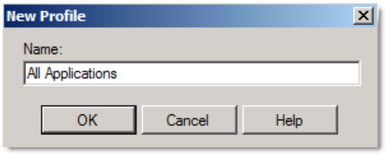
Group Profiles

Use the Group Profiles module to create group profiles for groups that share the same set of fields and permissions. This can make the user configuration process easier.

Creating Group Profiles

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

1. Select the Users & Groups module, and select Group Profiles.
2. Select New, name the profile, and click OK.



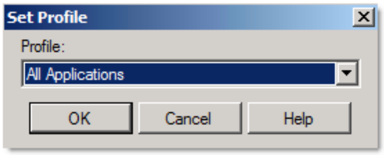
Name: All Applications

3. With the profile selected under Group profiles, click New under Groups and select the groups to include with the profile.
4. Click OK to close the dialog.

Assigning Group Profiles

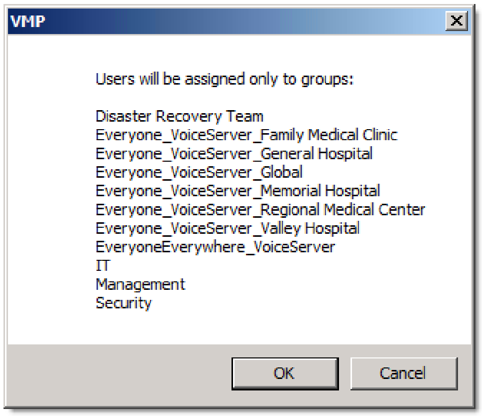
From the Users & Groups module, you can assign a group profile to a user. This makes the user a member of all groups in the group profile.

1. From the VMP Administrator, select Users & Groups > Users.
2. Click to highlight a user.
3. From the Member of tab, select Set Profile.
4. Use the dropdown list to select the profile, and click OK to close the dialog.



Profile: All Applications

5. Click OK to confirm the assigned groups.



Users will be assigned only to groups:

Disaster Recovery Team
Everyone_VoiceServer_Family Medical Clinic
Everyone_VoiceServer_General Hospital
Everyone_VoiceServer_Global
Everyone_VoiceServer_Memorial Hospital
Everyone_VoiceServer_Regional Medical Center
Everyone_VoiceServer_Valley Hospital
EveryoneEverywhere_VoiceServer
IT
Management
Security

Contacts

The Contacts module provides a secure messaging layer for system communications.

Contact options depend on the information provided by the administrator. Contact field options differ when the contact is entered using the Contact Sources or Distribution List option.

The Contacts module includes the following configuration views:

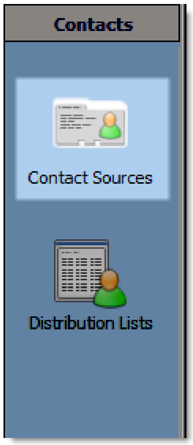
Table 22: Contacts module configuration views

View	Description
Contact Sources	Use the Contact Sources view to manually create a new user or to import contacts from a source.
Distribution Lists	Use the Distribution Lists view to create a new Contact Distribution List from contacts, users, and groups that are already available on the system.

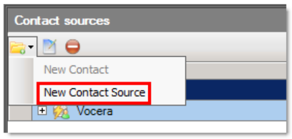
Importing Contacts From a Source

Use these steps to import contacts.

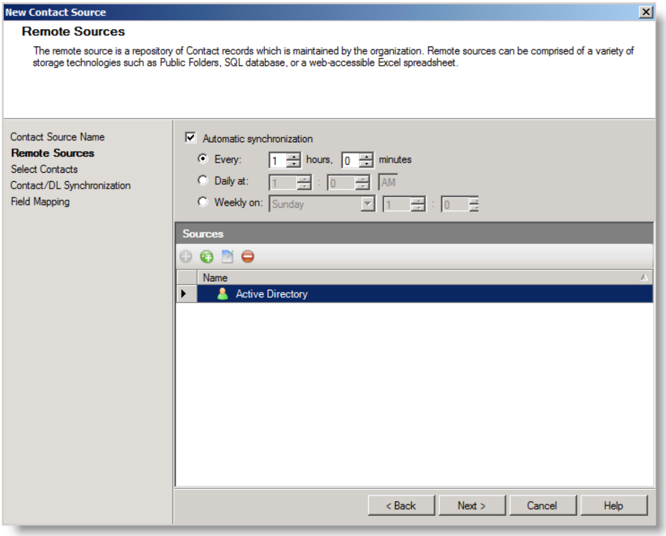
1. Select the Contacts module, and select Contact Sources.



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.



Remote Sources

The remote source is a repository of Contact records which is maintained by the organization. Remote sources can be comprised of a variety of storage technologies such as Public Folders, SQL database, or a web-accessible Excel spreadsheet.

☑ Automatic synchronization

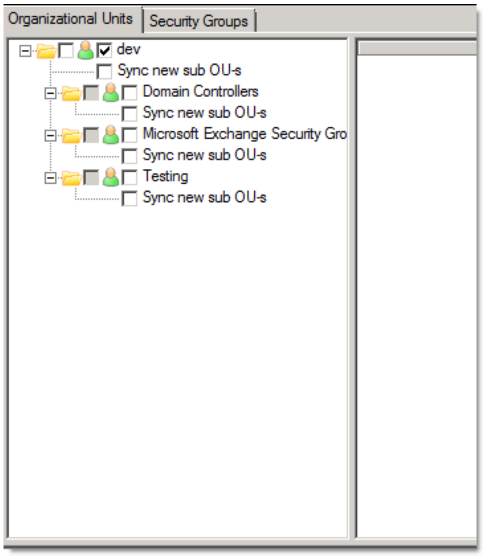
● Every: 1 hours, 0 minutes

○ Daily at: 1 : 0 AM

○ Weekly on: Sunday 1 : 0

Note: For more information about synchronizing from a contact source, see **Importing and Synchronizing Users and Contacts** on page 35.

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 **Defining Contact Fields** on page 104 and **Editing User Fields** on page 105.

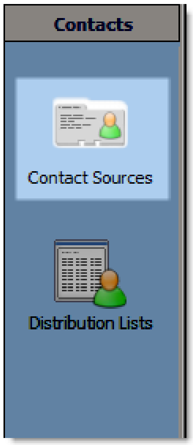
9. Confirm that the synchronization is successful and click OK to close the dialog.

Manually Adding a New Contact

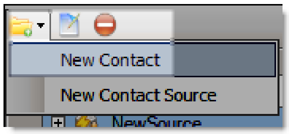
Use these steps to add a new contact from the VMP Administrator.

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

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



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



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

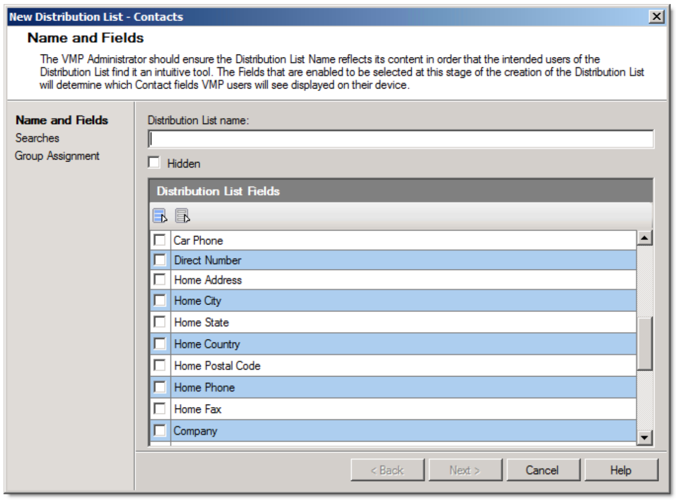
Note: To filter the list of contact sources, click Filter and select the filter criteria to use. The Filter icon changes color. To reset filtering, right-click Filter.

Creating a Contacts Distribution List

Use the following steps to create a Contacts Distribution List.

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 26 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.



New Distribution List - Contacts

Name and Fields

The VMP Administrator should ensure the Distribution List Name reflects its content in order that the intended users of the Distribution List find it an intuitive tool. The Fields that are enabled to be selected at this stage of the creation of the Distribution List will determine which Contact fields VMP users will see displayed on their device.

Distribution List name:

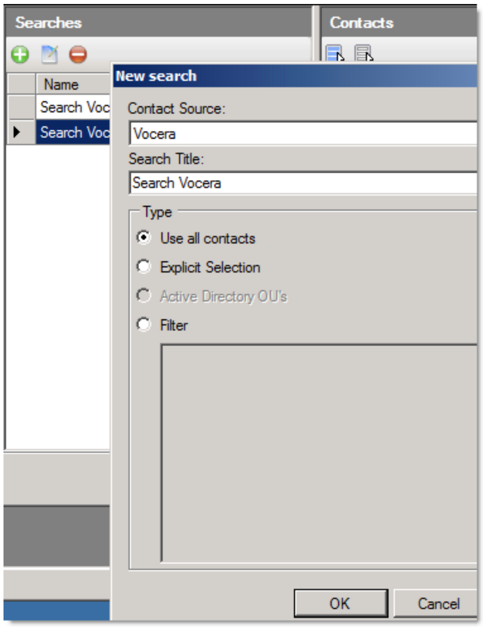
☐ Hidden

Distribution List Fields

☐ Car Phone
☐ Direct Number
☐ Home Address
☐ Home City
☐ Home State
☐ Home Country
☐ Home Postal Code
☐ Home Phone
☐ Home Fax
☐ Company

Tip: Click Select All to add all available fields.

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



Contact Source: Vocera

Search Title: Search Vocera

Type
- ● Use all contacts
- ○ Explicit Selection
- ○ Active Directory OU's
- ○ Filter

9. Select from the following options:

Table 23: 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.

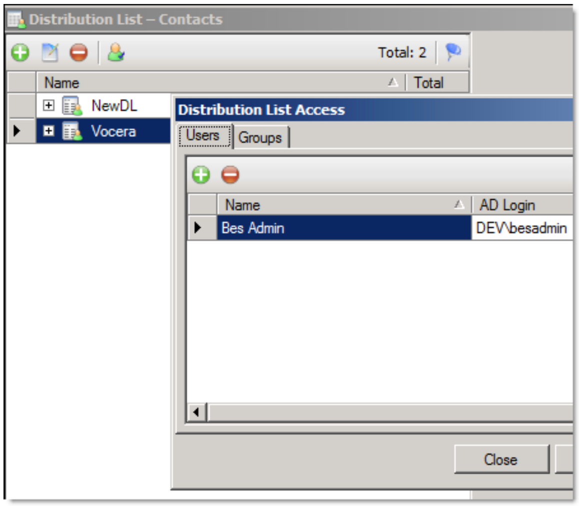
Tip: Filter for contacts with crucial fields (mobile phone, email address, etc.) to ensure you are adding only contacts with these fields populated.

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

Use the following steps to manage Contacts Distribution List access.

1. Select the Contacts module, and select Distribution Lists.
2. Select a list and click Manage Access to display the Distribution List Access dialog.



Name	AD Login
Bes Admin	DEV\besadmin

3. The Distribution List Access dialog allows you to perform the following tasks:

Table 24: 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.

Note: 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

Learn about using the Messaging module.

From this module, you can:

- Create and edit Messaging Templates.
- Create On-Call and Escalation Distribution Lists.

Note: Messages cannot be sent to groups. You must create Distribution Lists for Messaging users. For details on creating Distribution Lists, see **Distribution Lists** on page 91.

Messaging Templates

Messaging Templates enable users to quickly create frequently sent messages.

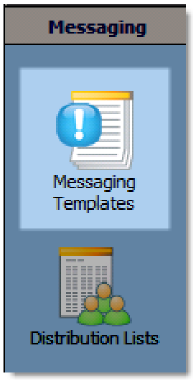
Templates can be assigned permissions based on Distribution Lists. They can be configured to send messages to Distribution Lists, which enables you to quickly send messages to a specific set of users.

Templates are made available for the smartphone client and the VMP Web Console.

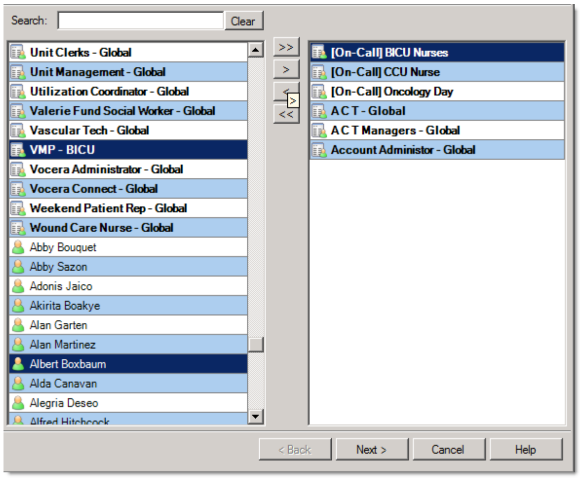
Creating Messaging Templates

You can create a Messaging Template to help you quickly create messages that you send frequently.

1. Open the VMP Administrator and select Messaging > Messaging Templates.



2. Click New.
3. Click to highlight each user or Distribution List that will receive a message when the template is used, and click > to add the users and Distribution Lists to the list of recipients. When the users and Distribution Lists are added, click Next.



- Unit Clerks - Global
- Unit Management - Global
- Utilization Coordinator - Global
- Valerie Fund Social Worker - Global
- Vascular Tech - Global
- VMP - BICU
- Vocera Administrator - Global
- Vocera Connect - Global
- Weekend Patient Rep - Global
- Wound Care Nurse - Global
- Abby Bouquet
- Abby Sazon
- Adonis Jaico
- Akirita Boakye
- Alan Garten
- Alan Martinez
- Albert Boxbaum
- Alda Canavan
- Alegria Deseo
- Alfred Hitchcock

- [On-Call] BICU Nurses
- [On-Call] CCU Nurse
- [On-Call] Oncology Day
- ACT - Global
- ACT Managers - Global
- Account Administor - Global

Note: The list of recipients can include only one Escalation Distribution List.

4. Enter the following template details, and click Next:

Table 25: Messaging Template options

Option	Description
Subject	The subject line of the message.
Message	The message text.
Priority	The message priority can be: • Urgent • High • Normal
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 26: 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: • 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:
   a. Click Add to add a response. Type the text of the response in the dialog box provided, and click OK.
   b. Click Edit to edit a response that you have created.
   c. Click Delete to delete a response that you have created.
   d. To rearrange the responses, click a response to highlight it. Click Move Up to move the response up in the list, or click Move Down to move the response down. Repeat until the responses are in the order that you want.
   e. Click Next when you have finished creating message options.
7. Click to highlight each user or group that can use the template, and click >. When the groups are added, click Finish.

Editing a Messaging Template

You can edit any Messaging Template that you have created.

1. In the VMP Administrator, select Messaging > Messaging Templates.
2. Highlight the Messaging Template that you want to edit and click Edit.
3. Add or remove users or Distribution Lists that will receive a message when this Messaging Template is used:
   a. To add a user or Distribution List, find the user or Distribution List in the left pane of the Edit Messaging Template dialog. Highlight the user or Distribution List, and click >.
   b. To remove a user or Distribution List, highlight it in the right pane of the Edit Messaging Template dialog and click <.

   When you have finished adding and removing users and Distribution Lists, click Next.
4. Edit the messaging options as needed, and click Next when finished.

   Note: For more information on these options, see **Creating Messaging Templates** on page 89.
5. If you selected Multiple Choice Responses, you can update the response options:
   a. Click Add to add a response. Type the text of the response in the dialog box provided, and click OK.
   b. Click Edit to edit a response that you have created.
   c. Click Delete to delete a response that you have created.

   d. To rearrange the responses, click a response to highlight it. Click Move Up to move the response up in the list, or click Move Down to move the response down. Repeat until the responses are in the order that you want.
   e. Click Next when you are finished updating responses.

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 change the permissions for any user or group that can send messages from 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:
   a. Click the Users tab to change permissions for users, or click the Groups tab to change permissions for groups.
   b. 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.

      The default administrator has Manage access permission on every Messaging Template.
   c. Click OK when done.
   d. Click Edit to edit the permissions of a user or group.
   e. Click Delete to delete from the list of users or groups with permissions.
4. Click Close to close the Messaging Template Permissions dialog box.

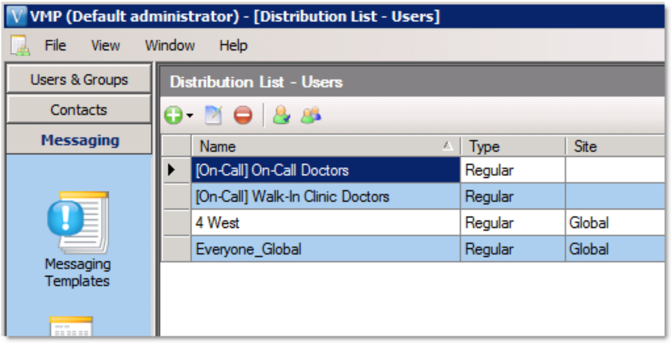
Distribution Lists

Distribution Lists (DLs) are created in the Messaging module of the VMP Administrator.

You can create the following types of DL:

- Regular or On-Call Distribution Lists: see **Creating a Regular or On-Call Distribution List** on page 92
- Escalation Distribution Lists: see **Creating an Escalation Distribution List** on page 95

The Distribution List - Users view shows a list of all available DLs.


VMP (Default administrator) - [Distribution List - Users]
File
View
Window
Help
Users & Groups
Contacts
Messaging
Messaging Templates
Distribution List - Users

Name	Type	Site
[On-Call] On-Call Doctors	Regular	
[On-Call] Walk-In Clinic Doctors	Regular	
4 West	Regular	Global
Everyone_Global	Regular	Global

Use this view to perform the following tasks:

Table 27: Distribution List view tasks

Task Icon	Description
⊕	Create a new Regular or Escalation DL.
✎	Edit the highlighted DL.
⊖	Delete the highlighted DL.
👤	Manage access to the highlighted DL.
👥	View all members of the highlighted DL.

This view includes the following fields:

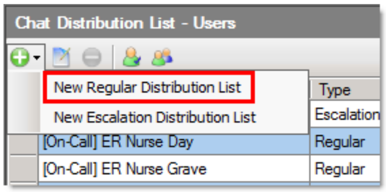
Table 28: Distribution List view fields

Field	Description
Name	The name of the DL. On-Call and Escalation DLs are marked with a bracketed indicator of the type of list. Sort the list by name using this field.
Type	Identifies the DL as Regular or Escalation. On-Call DLs are listed as regular DLs. Use this field to sort the list by Type.
Site	The site for this DL. 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 26 for more information on integrating with the Vocera Voice Server.
Enabled for Texting	Indicates messaging permissions with a Yes or No value.
Members	The total number of DL members.

Creating a Regular or On-Call Distribution List

Use the following steps to create a regular Distribution List (DL). You can specify that this list is to be an On-Call Distribution List.

1. Open the VMP Administrator application and select Messaging > Distribution Lists.
2. Click New ⊕ and select New Regular Distribution List.


Chat Distribution List - Users
New Regular Distribution List
New Escalation Distribution List
Type
Escalation
[On-Call] ER Nurse Day
Regular
[On-Call] ER Nurse Grave
Regular

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.

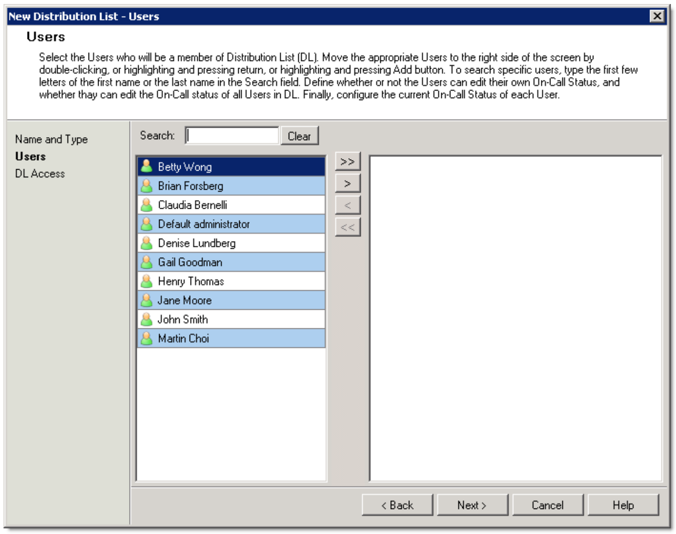
5. If this Distribution List is to be associated with a site, select the site from the Site dropdown list.

   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 26 for more information on integrating with the Vocera Voice Server.

6. Select Enable for Texting if you want this DL to be available to Messaging users.
7. 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: You can create On-Call DLs to manage shift assignments and Messaging communication coverage.

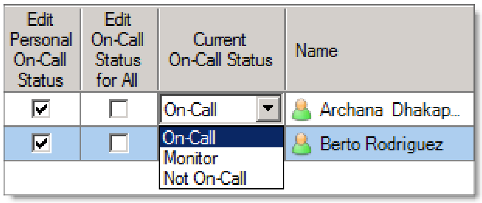
8. Select Hidden if this DL is to remain hidden. Vocera Collaboration Suite and VMP Web Console users can send messages to members of a hidden DL, but cannot send a message to the DL.
9. Select how users can be added to the DL. You can select either Add Users Manually or Create DL based on Active Directory structure.
10. Click Next.
11. If you have selected Add Users Manually:
    a. Type in the Search field to display only users whose names contain the search string. Click Clear to clear the search string.
    b. 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 >>.



Select the Users who will be a member of Distribution List (DL). Move the appropriate Users to the right side of the screen by double-clicking, or highlighting and pressing return, or highlighting and pressing Add button. To search specific users, type the first few letters of the first name or the last name in the Search field. Define whether or not the Users can edit their own On-Call Status, and whether thay can edit the On-Call status of all Users in DL. Finally, configure the current On-Call Status of each User.

    c. If the DL is an On-Call DL:

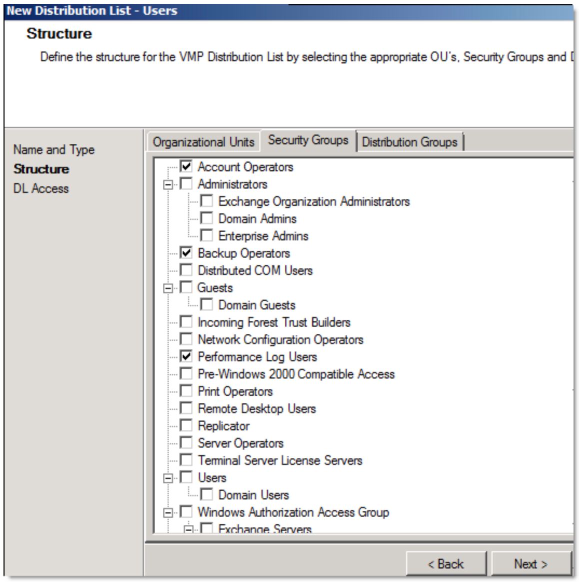
- Select Edit Personal On-Call Status to let users edit their own on-call status.
- Select Edit On-Call Status For All to let users manage the on-call status for all members of the DL.
- In the Current On-Call Status dropdown list, specify the on-call status for each user. Select Not On-Call, Monitor, or On-Call.



Edit Personal On-Call Status	Edit On-Call Status for All	Current On-Call Status	Name
☑	☐	On-Call	Archana Dhakap...
☑	☐	On-Call	Berto Rodriguez

d. 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.



New Distribution List - Users

Structure

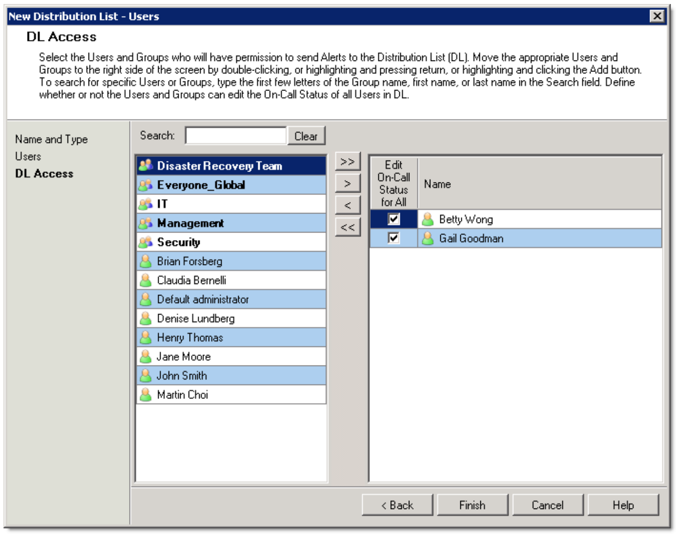
Define the structure for the VMP Distribution List by selecting the appropriate OU's, Security Groups and

- Name and Type
- **Structure**
- DL Access

Organizational Units | Security Groups | Distribution Groups

- ☑ Account Operators
- ☐ Administrators
  - ☐ Exchange Organization Administrators
  - ☐ Domain Admins
  - ☐ Enterprise Admins
- ☑ Backup Operators
- ☐ Distributed COM Users
- ☐ Guests
  - ☐ Domain Guests
- ☐ Incoming Forest Trust Builders
- ☐ Network Configuration Operators
- ☑ Performance Log Users
- ☐ Pre-Windows 2000 Compatible Access
- ☐ Print Operators
- ☐ Remote Desktop Users
- ☐ Replicator
- ☐ Server Operators
- ☐ Terminal Server License Servers
- ☐ Users
  - ☐ Domain Users
- ☐ Windows Authorization Access Group
  - ☐ Exchange Servers

13. The DL Access window appears, which lets you select the users and groups who will have permission to send messages to this DL.



New Distribution List - Users

DL Access

Select the Users and Groups who will have permission to send Alerts to the Distribution List (DL). Move the appropriate Users and Groups to the right side of the screen by double-clicking, or highlighting and pressing return, or highlighting and clicking the Add button. To search for specific Users or Groups, type the first few letters of the Group name, first name, or last name in the Search field. Define whether or not the Users and Groups can edit the On-Call Status of all Users in DL.

- Name and Type
- Users
- **DL Access**

Search: Clear

- **Disaster Recovery Team**
- **Everyone_Global**
- **IT**
- **Management**
- **Security**
- Brian Forsberg
- Claudia Bernelli
- Default administrator
- Denise Lundberg
- Henry Thomas
- Jane Moore
- John Smith
- Martin Choi

Edit On-Call Status for All	Name
☑	Betty Wong
☑	Gail Goodman

Type in the Search field to display only users whose names contain the search string. Click Clear to clear the search string.

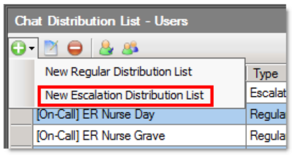
14. Click to highlight a user, and then click > to give the user permission to send a message to this Distribution List. You can click to highlight one or many users. To give all users permission to send messages, click >>.
15. If the new list is an On-Call Distribution List, select the Edit On-Call Status for All checkbox next to each user who is to be given permission to edit anyone's on-call status.
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.


Chat Distribution List - Users
New Regular Distribution List
New Escalation Distribution List
Type
Escalat
[On-Call] ER Nurse Day
Regula
[On-Call] ER Nurse Grave
Regula

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 29: Delivery route options

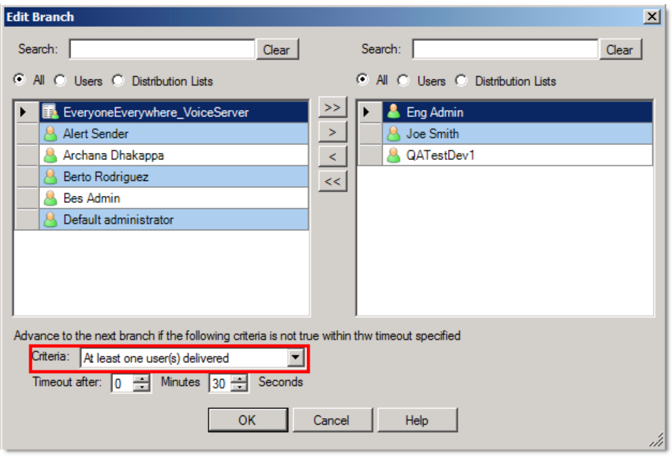
Option	Description
Deliver to all users	Deliver to all DL members.
Deliver only to Vocera Users who are present on the Wi-Fi network.	Messages sent to the DL are delivered only to active members who are currently logged onto the Vocera Voice Server and are not in DND mode.

6. Next, create the branches for the Escalation Distribution List:
    a. Click New to add a New Branch to the Escalation Distribution List. 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.
    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



EveryoneEverywhere_VoiceServer
Alert Sender
Archana Dhakappa
Berto Rodriguez
Bes Admin
Default administrator

Eng Admin
Joe Smith
QATestDev1

Advance to the next branch if the following criteria is not true within thw timeout specified

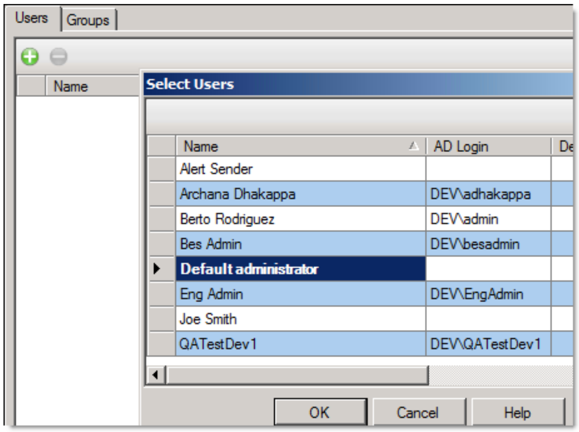
Criteria: At least one user(s) delivered

Timeout after: 0 Minutes 30 Seconds

f. Set the timeout value and click OK to continue.

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.



Name	AD Login	De
Alert Sender		
Archana Dhakappa	DEV\adhakappa	
Berto Rodriguez	DEV\admin	
Bes Admin	DEV\besadmin	
Default administrator		
Eng Admin	DEV\EngAdmin	
Joe Smith		
QATestDev1	DEV\QATestDev1	

8. Click the Users tab to add a user to the access list, or click Groups to add a group:

   a. Click ⊕ to display a list of users or groups.

   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 92.
    - If you are editing an Escalation Distribution List, see **Creating an Escalation Distribution List** on page 95.

Note: To filter the list of Distribution Lists, click Filter and enter the filtering criterion to use. 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.
4. 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.
5. 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.
6. When you have finished updating user access, click Close.

Note: 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.

4. 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.

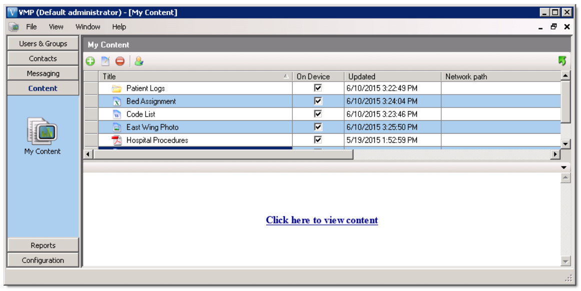
Content is uploaded and managed by the administrator. When a file is uploaded to the VMP Server, the title and upload date are posted to the main screen of the console. VMP supports the following file types:

- HTML file
- Image file (JPEG, GIF, BMP and PNG)
- PDF file
- Microsoft Word document
- Text
- Audio and video

To support Word, Excel, and PDF, the VMP Server must have Microsoft Word, Excel, and Adobe Acrobat Reader installed in order to 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.

Note: Streaming audio and video cannot be played if access to the VMP Server is through the Vocera Smartphone Proxy.

The My Content view provides a list of the current documentation in the configured hierarchy.



Title	On Device	Updated	Network path
Patient Logs	☑	6/10/2015 3:22:49 PM	
Bed Assignment	☑	6/10/2015 3:24:04 PM	
Code List	☑	6/10/2015 3:23:46 PM	
East Wing Photo	☑	6/10/2015 3:25:50 PM	
Hospital Procedures	☑	5/19/2015 1:52:59 PM	

Features of this view include:

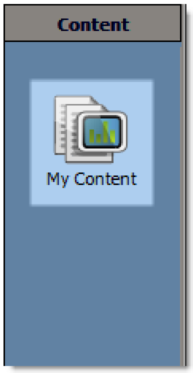
- Content view window
- Activate or deactivate device presence
- Content update timestamp
- Network path information

Note: To refresh the list of available content displayed in the Content module, click Refresh.

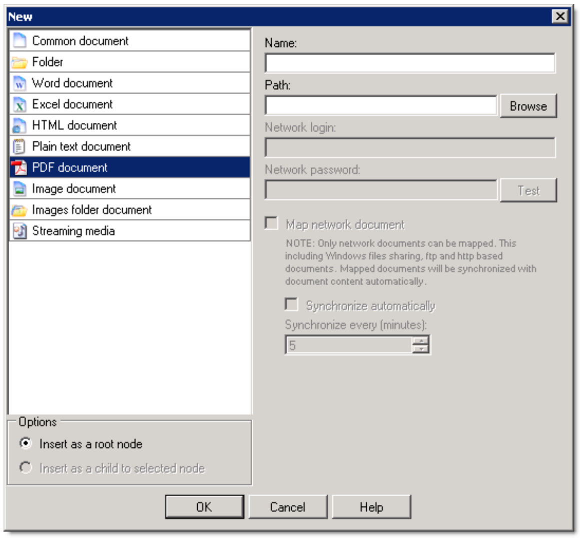
Adding Content

Use these steps to add content using the VMP Administrator.

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: Only network documents can be mapped. This including Windows files sharing, ftp and http based documents. Mapped documents will be synchronized with document content automatically.

Options

● Insert as a root node

○ Insert as a child to selected node

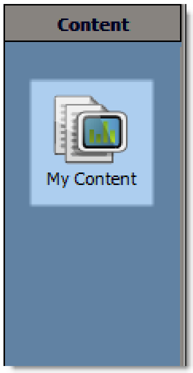
Note: The Name field contains the document name, and it auto-populates based on the selected document. If you enter a name in the Name field, it will persist.

5. If the document resides on a network that requires credentials, 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.
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.

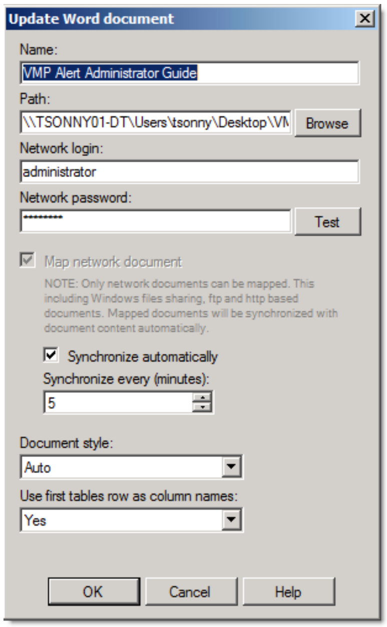
Updating Content

Use the following steps to update content.

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.



Name: VMP Alert Administrator Guide

Path: \\TSONNY01-DT\Users\tsonny\Desktop\VM

Network login: administrator

Network password: ********

☑ Map network document

NOTE: Only network documents can be mapped. This including Windows files sharing, ftp and http based documents. Mapped documents will be synchronized with document content automatically.

☑ Synchronize automatically

Synchronize every (minutes): 5

Document style: Auto

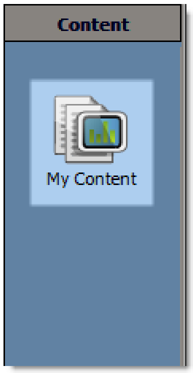
Use first tables row as column names: Yes

Assigning Document Permissions

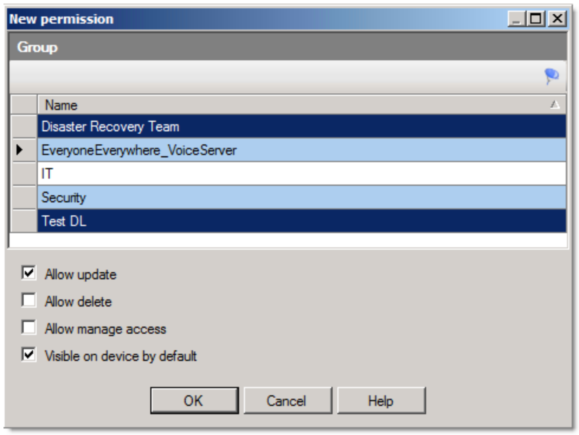
Use the VMP Administrator to manage permissions for files uploaded to the VMP Server.

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



Disaster Recovery Team
EveryoneEverywhere_VoiceServer
IT
Security
Test DL

☑ Allow update
☐ Allow delete
☐ Allow manage access
☑ Visible on device by default

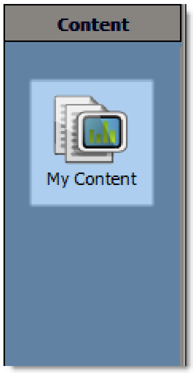
6. Click OK.

To filter the list of entries, click Filter. To reset filtering, right-click Filter.

Deleting Content

Use these steps to 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

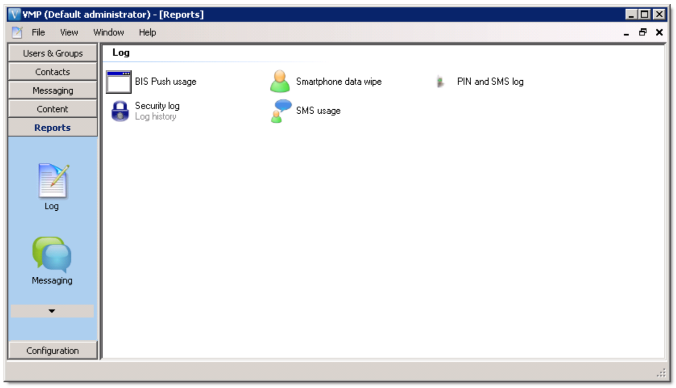
The Reports module gives Vocera administrators the ability to customize reports for organizational requirements such as audits and quality of service. Administrators can generate a report at any time and filter specific messaging details.

The following categories of reports are available:

- Log
- Messaging
- Transmit Status

Creating Logging Reports

In the Reports module, selecting the Log icon displays the logging reports that can be generated.



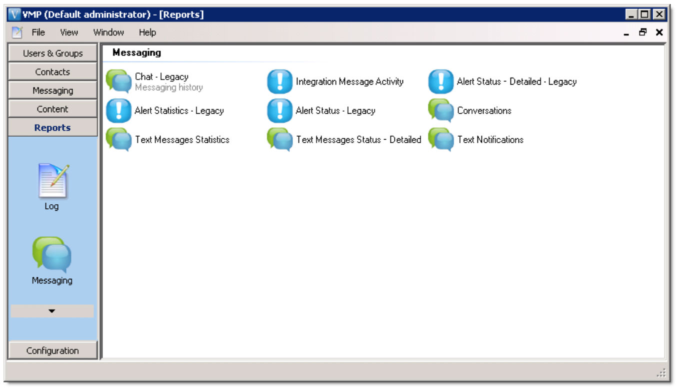
The following Log reports can be generated:

Table 30: 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.
SMS usage	Shows the SMS usage of a device.

Creating Messaging Reports

In the Reports module, selecting the Messaging icon lets you display reports that list the messaging history, statuses, and statistics for the VMP Server.



The following Messaging reports can be generated:

Table 31: 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.
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. Select the user from the user filter that appears when the report screen is displayed.
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.

Creating Transmit Status Reports

In the Reports module, selecting the Transmit Status icon lets you display reports that list the status of Chat messages and content sent from the VMP Server.

The following Transmit Status reports can be generated:

Table 32: 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.

Configuration

The VMP Administrator Configuration module includes the views described here.

Table 33: 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 Systems Options, see **Configuration Options Reference** on page 135. For more information on Wireless Gateways, see **Configuring Wireless Gateways** on page 22.

System Options

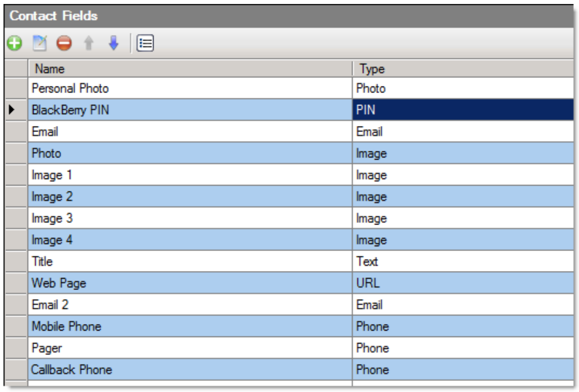
The System Options control the behavior of the VMP Server and the VMP Administrator.

For more information on system options, see **VMP Administrator Configuration Options** on page 135.

Defining 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

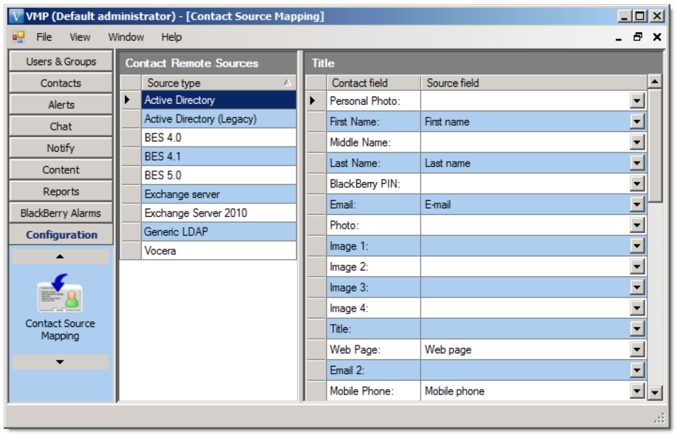
The Contact Fields view includes the following options:

Table 34: 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.

Editing Contact Fields

Use the VMP Administrator Contact Source Mapping module to edit contact fields.



Source type
Active Directory
Active Directory (Legacy)
BES 4.0
BES 4.1
BES 5.0
Exchange server
Exchange Server 2010
Generic LDAP
Vocera

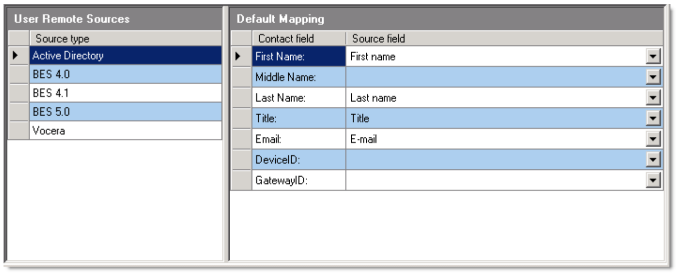
Contact field	Source field
Personal Photo:	
First Name:	First name
Middle Name:	
Last Name:	Last name
BlackBerry PIN:	
Email:	E-mail
Photo:	
Image 1:	
Image 2:	
Image 3:	
Image 4:	
Title:	
Web Page:	Web page
Email 2:	
Mobile Phone:	Mobile phone

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.

Editing User Fields

Use the VMP Administrator User Source Mapping module to map VMP fields to fields from the import source.



Source type
Active Directory
BES 4.0
BES 4.1
BES 5.0
Vocera

Contact field	Source field
First Name:	First name
Middle Name:	
Last Name:	Last name
Title:	Title
Email:	E-mail
DeviceID:	
GatewayID:	

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 35: Plugin configuration support

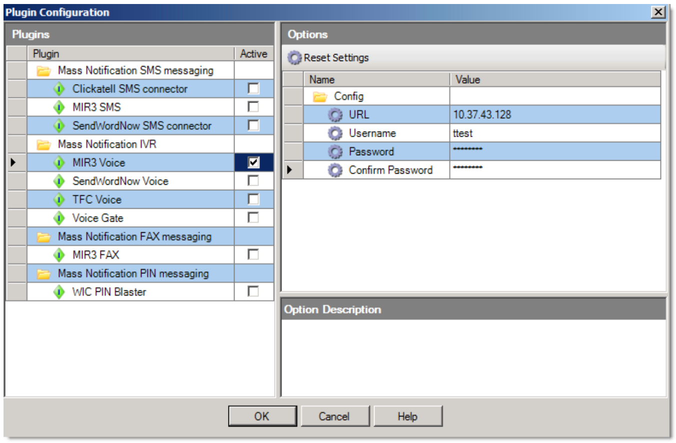
Plugin	Settings
Clickatell SMS connector	Enter the following settings: • AppID • User • Password • Confirm Password • From
MIR3 SMS	Enter the following settings: • URL • Username • Password • Confirm Password
SendWordNow SMS connector	Enter the following settings: • Login • Password • Confirm Password
MIR3 Voice	Enter the following settings: • URL • Username • Password • Confirm Password
SendWordNow Voice	Enter the following settings: • Login • Password • Confirm Password
TFC Voice	Enter the following settings: • Username • Password • Confirm Password • cli_id • user_id • caller_id
Voice Gate	Enter the following settings: • Client Name • Client ID • Confirm Client ID • Display Number

Plugin	Settings
MIR3 Fax	Enter the following settings: • Company • URL • Username • Password • Confirm Password
WIC PIN Blaster	Enter the following settings: • Server • Login • Password • Confirm Password

Using the Plugin Configuration Module

Use the following steps to configure a plugin.

1. From the VMP Administrator, select Configuration > Plugin Configuration.
2. Click the Active checkbox for the plugin you want to configure.



Plugin	Active
Mass Notification SMS messaging	
Clickatell SMS connector	☐
MIR3 SMS	☐
SendWordNow SMS connector	☐
Mass Notification IVR	
MIR3 Voice	☑
SendWordNow Voice	☐
TFC Voice	☐
Voice Gate	☐
Mass Notification FAX messaging	
MIR3 FAX	☐
Mass Notification PIN messaging	
WIC PIN Blaster	☐

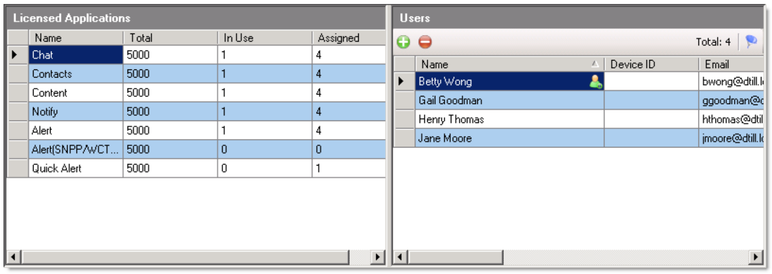
Name	Value
Config	
URL	10.37.43.128
Username	ttest
Password	*********
Confirm Password	*********

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.

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.



Name	Total	In Use	Assigned
Chat	5000	1	4
Contacts	5000	1	4
Content	5000	1	4
Notify	5000	1	4
Alert	5000	1	4
Alert(SNPP/WCT...	5000	0	0
Quick Alert	5000	0	1

Name	Device ID	Email
Betty Wong		bwong@dtill.l
Gail Goodman		ggoodman@
Henry Thomas		hthomas@dtil
Jane Moore		jmoore@dtill.l

The VMP Web Console

Learn about the VMP Web Console features.

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.

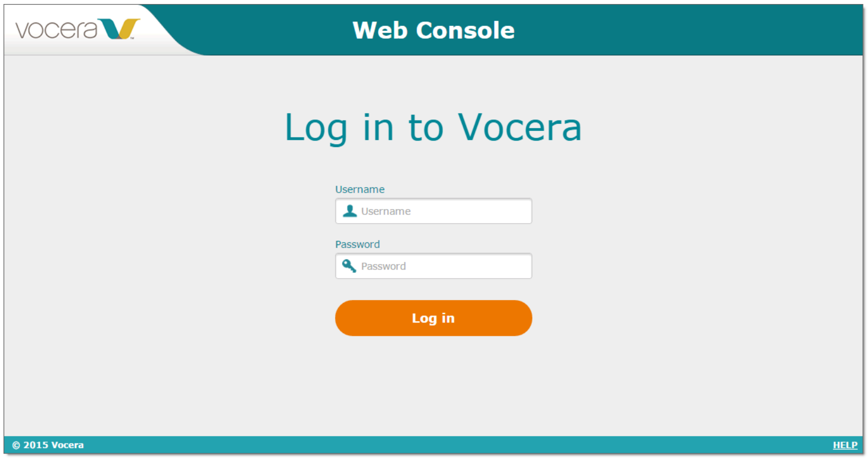
Users are assigned access to the VMP Web Console in the VMP Administrator. For details about granting users access to the VMP Web Console, see **Granting Existing Users Access to the VMP Web Console** on page 122.

Browser Requirements

The VMP Web Console is supported on Internet Explorer version 9 and later.

Logging into the VMP Web Console

To use the VMP Web Console, you must log in.

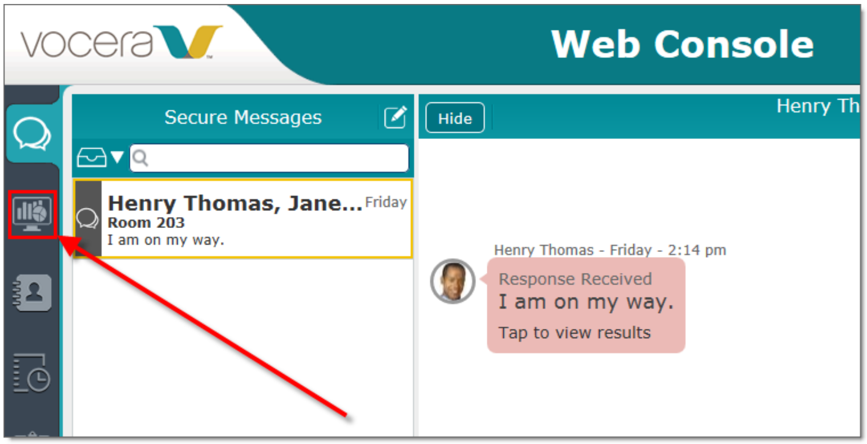


1. In the Username field, type your username.
2. In the Password field, type the password for your username.
3. Click Log in to log in to the VMP Web Console.

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 .

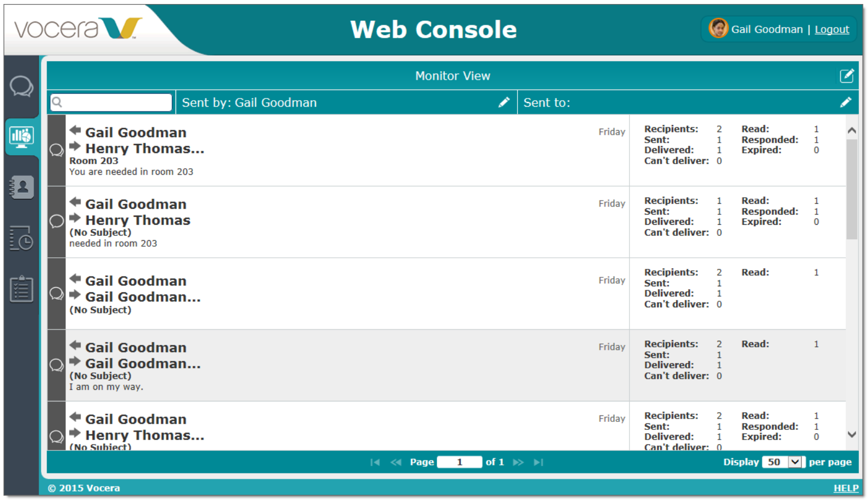


Henry Thomas, Jane... Friday
Room 203
I am on my way.

Henry Thomas - Friday - 2:14 pm
Response Received
I am on my way.
Tap to view results

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 123 for more information on granting permission to view messages.

The Monitor View lists each message.



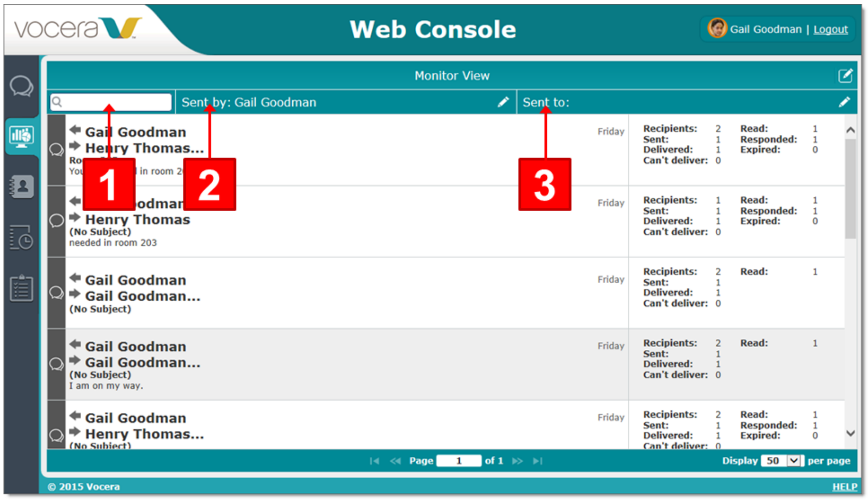
Sent by: Gail Goodman
Sent to:

Gail Goodman **Henry Thomas...** **Room 203** You are needed in room 203	Friday	**Recipients:** 2 **Sent:** 1 **Delivered:** 1 **Can't deliver:** 0	**Read:** 1 **Responded:** 1 **Expired:** 0
Gail Goodman **Henry Thomas** **(No Subject)** needed in room 203	Friday	**Recipients:** 1 **Sent:** 1 **Delivered:** 1 **Can't deliver:** 0	**Read:** 1 **Responded:** 1 **Expired:** 0
Gail Goodman **Gail Goodman...** **(No Subject)**	Friday	**Recipients:** 2 **Sent:** 1 **Delivered:** 1 **Can't deliver:** 0	**Read:** 1
Gail Goodman **Gail Goodman...** **(No Subject)** I am on my way.	Friday	**Recipients:** 2 **Sent:** 1 **Delivered:** 1 **Can't deliver:** 0	**Read:** 1
Gail Goodman **Henry Thomas...** **(No Subject)**	Friday	**Recipients:** 2 **Sent:** 1 **Delivered:** 1 **Can't deliver:** 0	**Read:** 1 **Responded:** 1 **Expired:** 0

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.



Sent by: Gail Goodman

Sent to:

Gail Goodman
Henry Thomas...
Friday
Recipients: 2 Sent: 1 Delivered: 1 Can't deliver: 0
Read: 1 Responded: 1 Expired: 0

Henry Thomas
(No Subject)
needed in room 203
Friday
Recipients: 1 Sent: 1 Delivered: 1 Can't deliver: 0
Read: 1 Responded: 1 Expired: 0

Gail Goodman
Gail Goodman...
(No Subject)
Friday
Recipients: 2 Sent: 1 Delivered: 1 Can't deliver: 0
Read: 1

Gail Goodman
Gail Goodman...
(No Subject)
I am on my way.
Friday
Recipients: 2 Sent: 1 Delivered: 1 Can't deliver: 0
Read: 1

Gail Goodman
Henry Thomas...
(No Subject)
Friday
Recipients: 2 Sent: 1 Delivered: 1 Can't deliver: 0
Read: 1 Responded: 1 Expired: 0

1	Use the search box to search for messages by: • Sender • Recipient • Subject • Keyword (in the message subject)
2	The Sent by field. Click ✎ to create Sent By filters.
3	The Sent to field. Click ✎ to create Sent To filters.

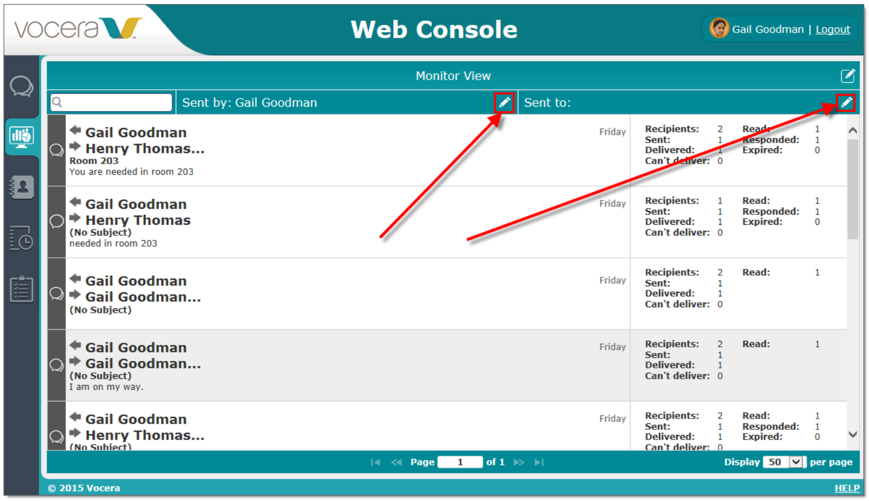
For more information on using the Sent By and Sent To filters, see **Monitor View Filtering** on page 110.

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 123 for more information on granting permission to view messages.

Monitor View Filtering

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:
   a. Click ✎ in the Sent by field to edit the Sent By filter.
   b. Click ✎ in the Sent to field to edit the Sent To filter.



Sent by: Gail Goodman
Sent to:

Gail Goodman
Henry Thomas...
Room 203
You are needed in room 203
Friday
Recipients: 2 Read: 1
Sent: 1 Responded: 1
Delivered: 1 Expired: 0
Can't deliver: 0

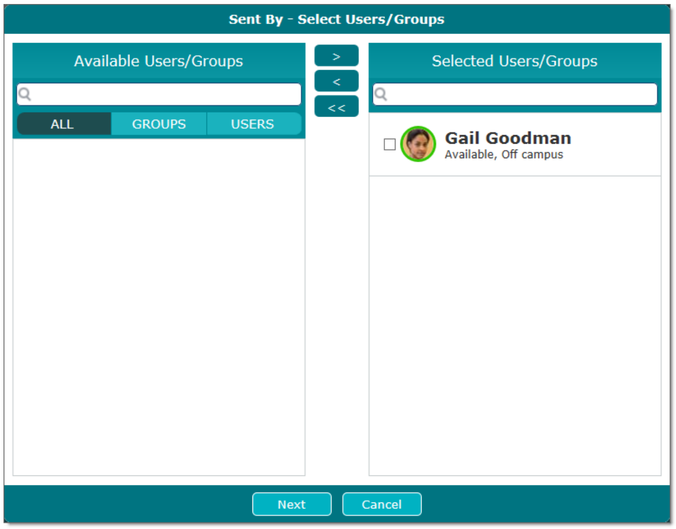
Gail Goodman
Henry Thomas
(No Subject)
needed in room 203
Friday
Recipients: 1 Read: 1
Sent: 1 Responded: 1
Delivered: 1 Expired: 0
Can't deliver: 0

Gail Goodman
Gail Goodman...
(No Subject)
Friday
Recipients: 2 Read: 1
Sent: 1
Delivered: 1
Can't deliver: 0

Gail Goodman
Gail Goodman...
(No Subject)
I am on my way.
Friday
Recipients: 2 Read: 1
Sent: 1
Delivered: 1
Can't deliver: 0

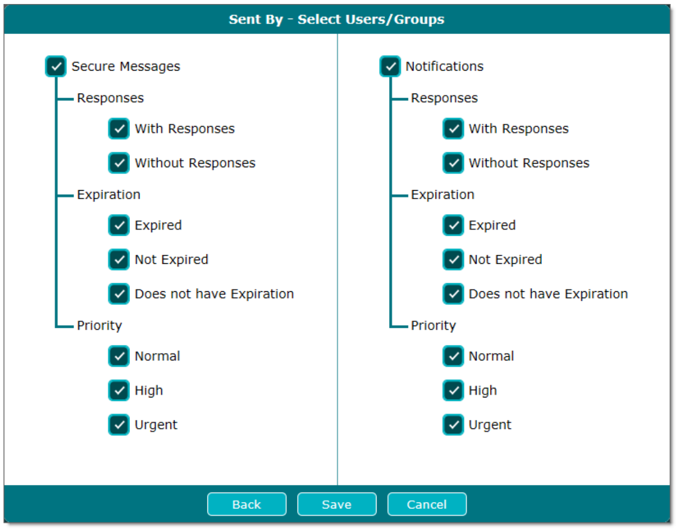
Gail Goodman
Henry Thomas...
(No Subject)
Friday
Recipients: 2 Read: 1
Sent: 1 Responded: 1
Delivered: 1 Expired: 0
Can't deliver: 0

2. In the Select Users/Groups dialog box, select the checkboxes of the users and groups to include in the filter. Click > to add these users and groups.



☐ Gail Goodman
Available, Off campus

3. To remove users and groups from the filter, click <. To remove all users and groups, click <<.
4. Click Next.
5. 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.



- ☑ Secure Messages
  - Responses
    - ☑ With Responses
    - ☑ Without Responses
  - Expiration
    - ☑ Expired
    - ☑ Not Expired
    - ☑ Does not have Expiration
  - Priority
    - ☑ Normal
    - ☑ High
    - ☑ Urgent
- ☑ Notifications
  - Responses
    - ☑ With Responses
    - ☑ Without Responses
  - Expiration
    - ☑ Expired
    - ☑ Not Expired
    - ☑ Does not have Expiration
  - Priority
    - ☑ Normal
    - ☑ High
    - ☑ Urgent

6. 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.

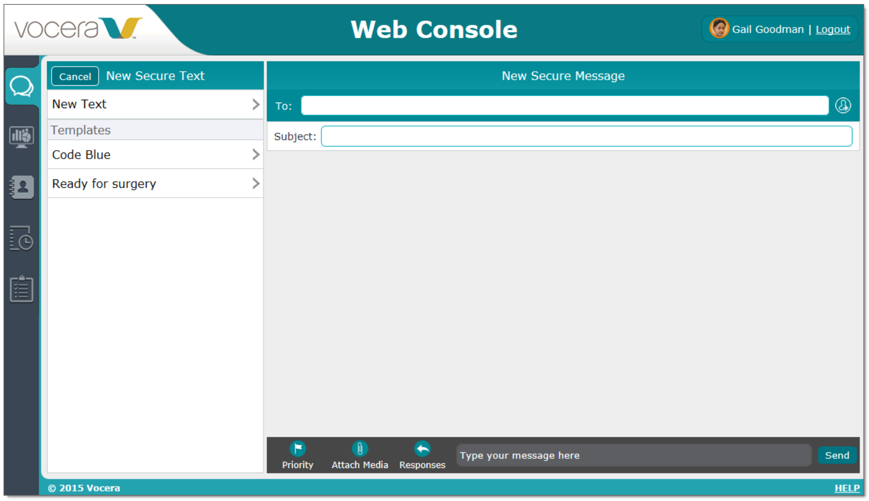
Note: The text of a message can be up to 3000 characters long, and the subject header can contain up to 512 characters. Any ASCII character can be included, but emojis are not supported.

Sending a Message from the VMP Web Console

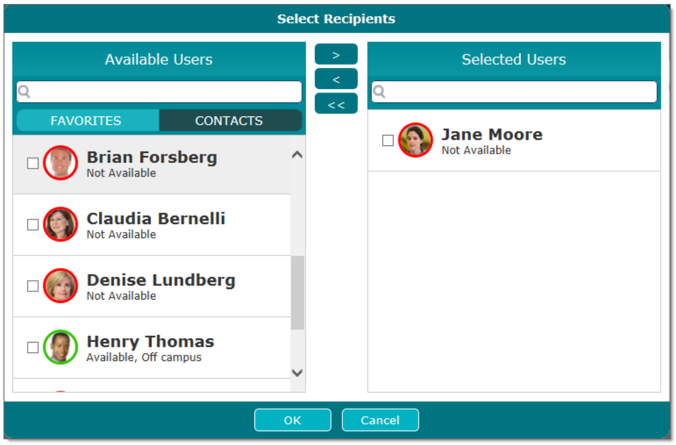
You can use the VMP Web Console to send a message to any user or Distribution List.

Note: If the message has more than 50 recipients, it is defined to be a Mass Notification. See **Creating a Mass Notification** on page 115 for details.

1. Open the VMP Web Console from your Web browser.
2. Select the Message icon and click the Compose icon.
3. To use a message Template, select it from the Templates list. If no Templates are available, or if you do not want to use a Template, select New Text.



4. To add one or more message recipients, either type the recipient name in the To: field, or click 👤 to select a Distribution List or user recipient.
5. If you have clicked 👤, in the Select Recipients dialog box, select the checkboxes of the users and Distribution Lists to include as recipients in the filter. Click > to add these recipients.



To remove recipients from the recipient list, click <. To remove all recipients, click <<.

6. If your message has a subject, type the subject in the Subject field.
7. 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 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.

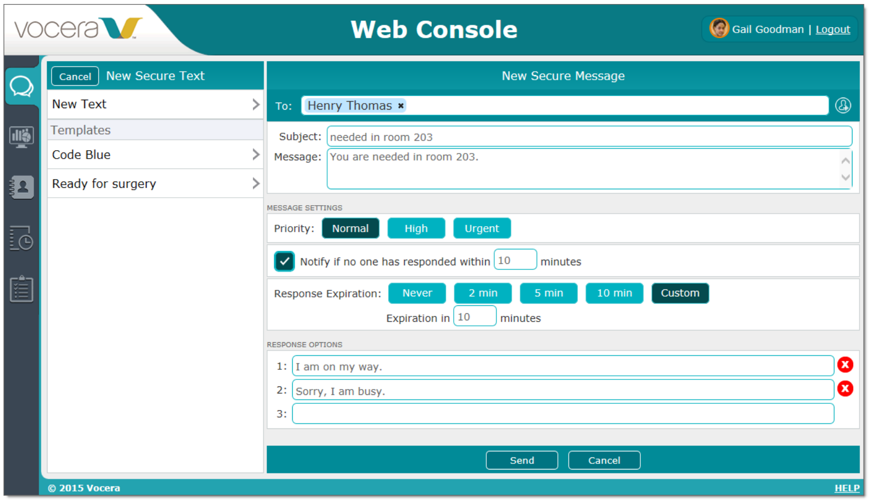
8. Do one of the following:
   a. To send a text message, type the message text in the field at the bottom of the screen and click Send.
   b. To send a photo, click 📎 Attach Media and select the image that you want to send.

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 114 for more details.

Sending a Message That Requires a Response

You can send a message that requires the recipient to provide a response.

1. Open the VMP Web Console from your Web browser.
2. Select the Message icon and click the Compose icon.
3. To use a message Template, select it from the Templates list. If no Templates are available, or if you do not want to use a Template, select New Text.
4. To add one or more message recipients, either type the recipient name in the To: field, or click to select a Distribution List or user recipient.
5. Click Responses to display the screen for sending a message with a response.



To: Henry Thomas

Subject: needed in room 203

Message: You are needed in room 203.

MESSAGE SETTINGS

Priority: Normal High Urgent

☑ Notify if no one has responded within 10 minutes

Response Expiration: Never 2 min 5 min 10 min Custom

Expiration in 10 minutes

RESPONSE OPTIONS

1: I am on my way.

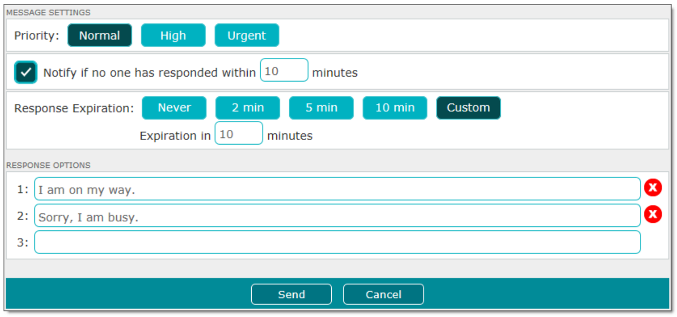
2: Sorry, I am busy.

3:

6. Type text in the Subject and Message fields (if they have not already been provided by the Template).

Note: A message must have text in the Message field.

7. Configure the following options, and click Send.



MESSAGE SETTINGS

Priority: Normal High Urgent

☑ Notify if no one has responded within 10 minutes

Response Expiration: Never 2 min 5 min 10 min Custom

Expiration in 10 minutes

RESPONSE OPTIONS

1: I am on my way.

2: Sorry, I am busy.

3:

Table 36: Web Console message options

Option	Description
Priority	One of the following: • Normal (the default) • High • Urgent See **Sending a Message from the VMP Web Console** on page 112 for details on how these priority levels are handled in the VCS app. **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.
Notify if no one has responded	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. • 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	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.
Response Options	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 ⊗.

8. 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 112.

Creating a Mass Notification

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.

Templates

Templates are predefined messages designed to help users quickly send important communications. Templates are created and managed from the VMP Administrator.

Templates can be:

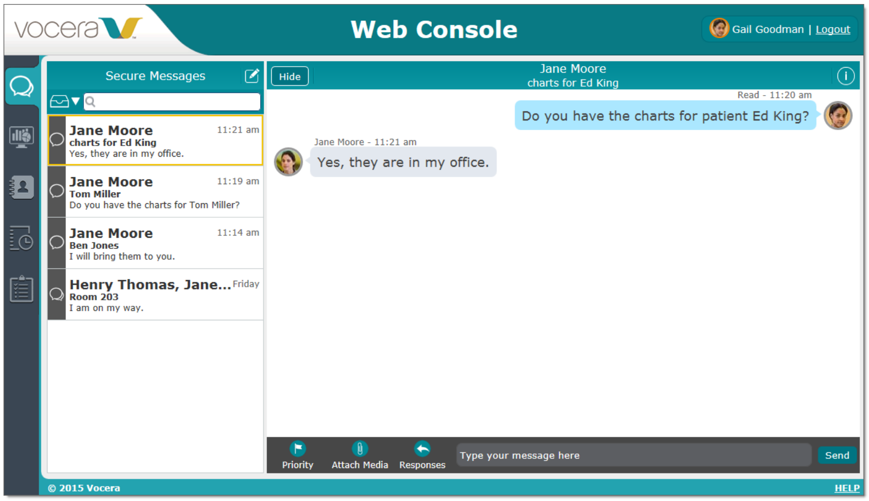
- Assigned permissions based on group memebership
- Configured to allow the user to edit the message and delivery parameters from the client
- Assigned to users and groups for frequently communicating important messages

For information about creating Templates, see **Creating Messaging Templates** on page 89.

Continuing a Message Conversation

After you have sent a secure message in the VMP Web Console, you can continue a conversation with the recipients of the message.

1. Select the Message icon.
2. From the list of messages in the Secure Messages pane, select the message. The message is displayed in the pane at the right.



Jane Moore 11:21 am
charts for Ed King
Yes, they are in my office.

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.

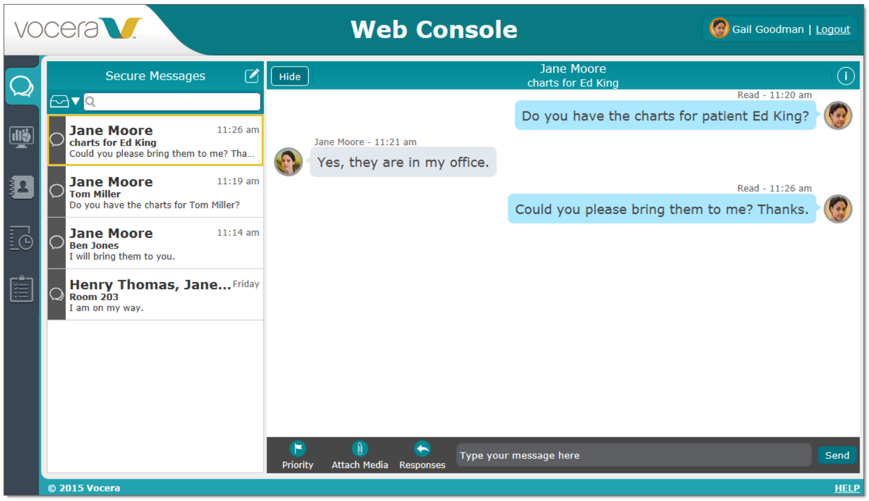
Henry Thomas, Jane... Friday
Room 203
I am on my way.

Jane Moore
charts for Ed King

Read - 11:20 am
Do you have the charts for patient Ed King?

Jane Moore - 11:21 am
Yes, they are in my office.

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.



Jane Moore 11:26 am
charts for Ed King
Could you please bring them to me? Tha...

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.

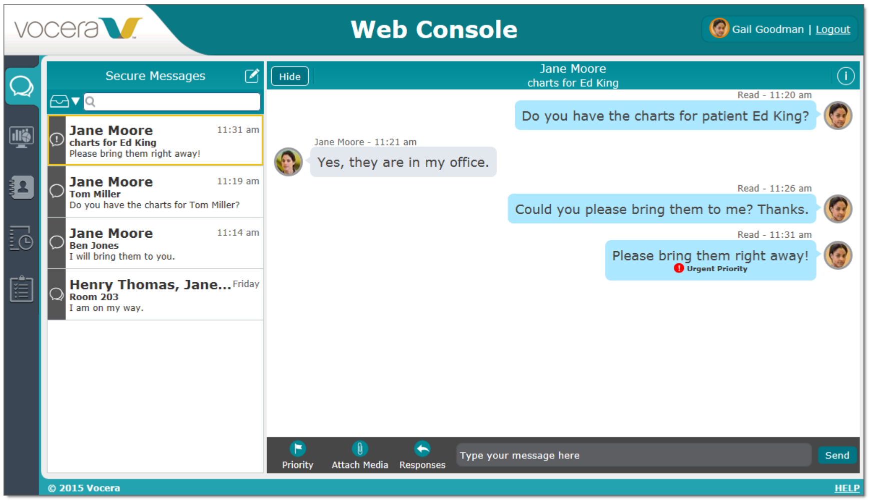
Jane Moore
charts for Ed King

Read - 11:20 am
Do you have the charts for patient Ed King?

Jane Moore - 11:21 am
Yes, they are in my office.

Read - 11:26 am
Could you please bring them to me? Thanks.

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.



Jane Moore 11:31 am
charts for Ed King
Please bring them right away!

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.

Jane Moore
charts for Ed King

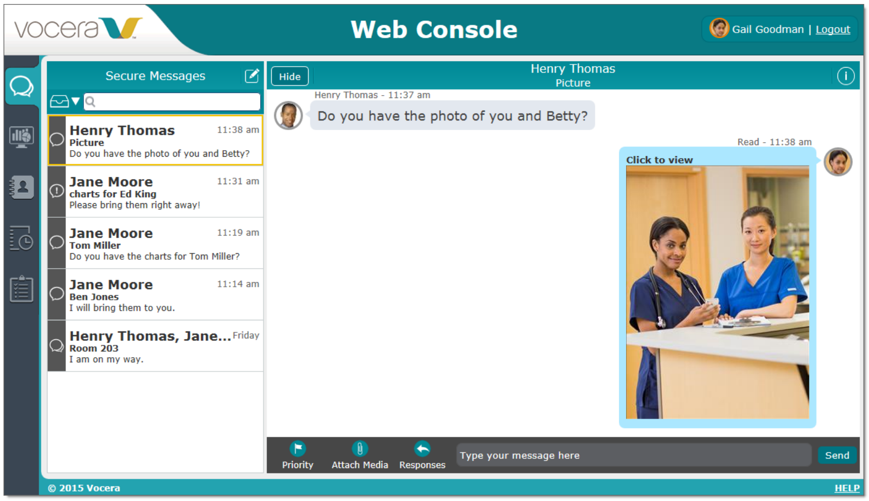
Read - 11:20 am
Do you have the charts for patient Ed King?

Jane Moore - 11:21 am
Yes, they are in my office.

Read - 11:26 am
Could you please bring them to me? Thanks.

Read - 11:31 am
Please bring them right away!
Urgent Priority

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.



Henry Thomas 11:38 am
Picture
Do you have the photo of you and Betty?

Jane Moore 11:31 am
charts for Ed King
Please bring them right away!

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.

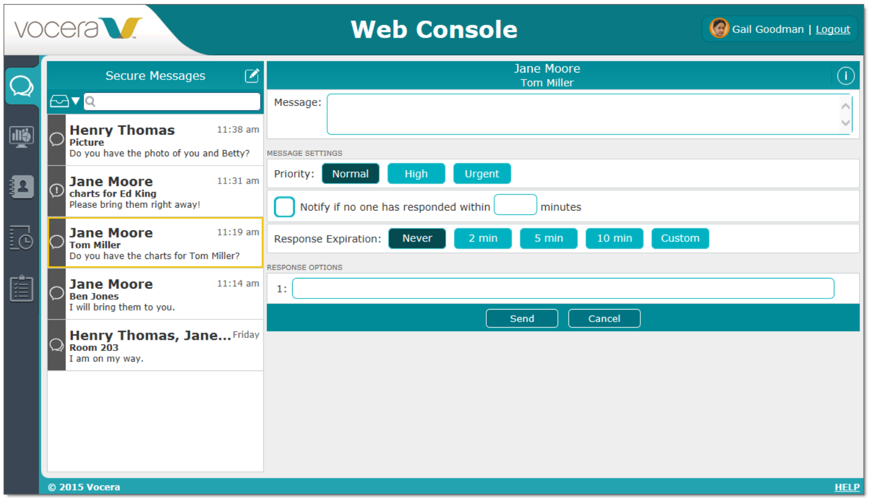
Henry Thomas
Picture

Henry Thomas - 11:37 am
Do you have the photo of you and Betty?

Read - 11:38 am

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.



Henry Thomas 11:38 am
Picture
Do you have the photo of you and Betty?

Jane Moore 11:31 am
charts for Ed King
Please bring them right away!

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.

Jane Moore
Tom Miller

Message:

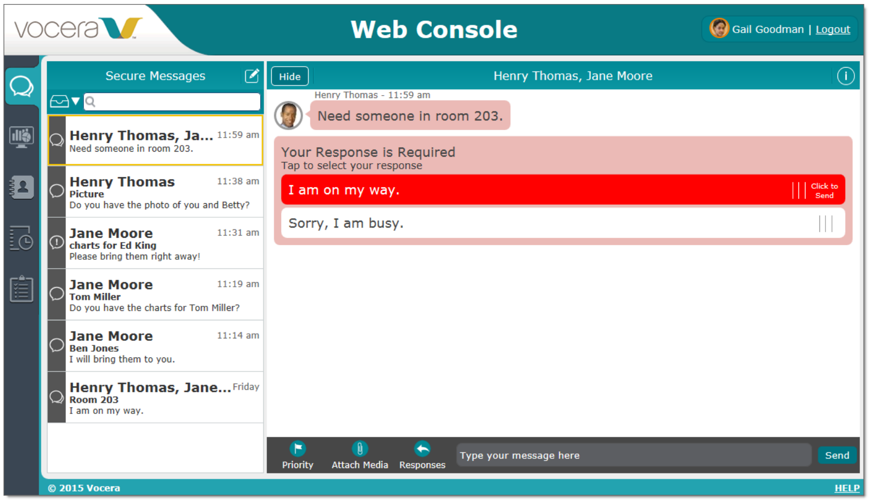
Priority: Normal High Urgent

☐ Notify if no one has responded within ___ minutes

Response Expiration: Never 2 min 5 min 10 min Custom

1:

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.



Henry Thomas, Ja... 11:59 am
Need someone in room 203.

Henry Thomas 11:38 am
Picture
Do you have the photo of you and Betty?

Jane Moore 11:31 am
charts for Ed King
Please bring them right away!

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.

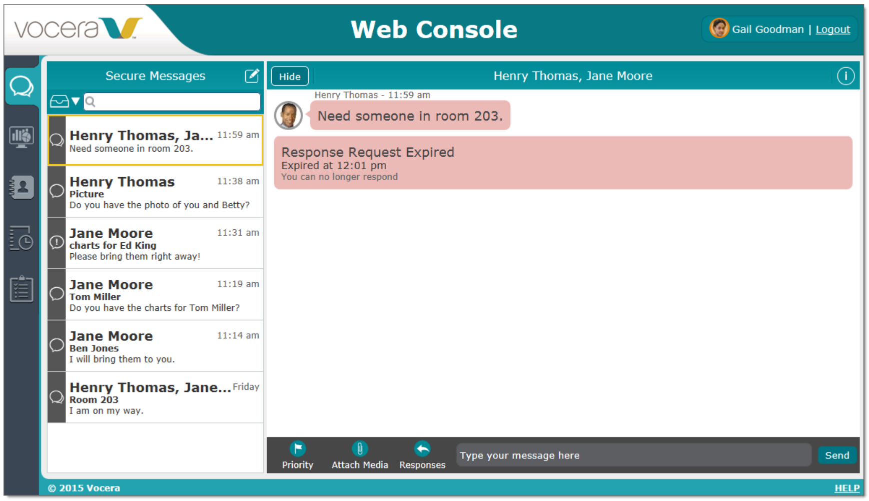
Henry Thomas - 11:59 am
Need someone in room 203.

Your Response is Required
Tap to select your response

I am on my way. Click to Send

Sorry, I am busy.

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:



Henry Thomas, Ja... 11:59 am
Need someone in room 203.

Henry Thomas 11:38 am
Picture
Do you have the photo of you and Betty?

Jane Moore 11:31 am
charts for Ed King
Please bring them right away!

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.

Henry Thomas - 11:59 am
Need someone in room 203.

Response Request Expired
Expired at 12:01 pm
You can no longer respond

If you are having more than one conversation, use the pane at the left to switch from one session to another.

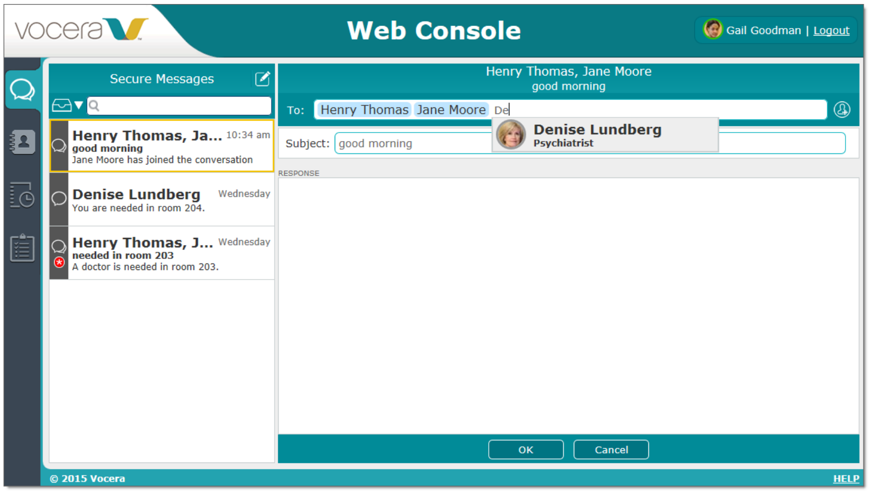
To display the current message delivery status, click on any text that you have sent in a conversation.

Click on a profile picture to display the contact status information for that person.

Adding a User to a Message Conversation

You can add additional users to an existing message conversation.

1. In the message conversation, click ⓘ.
2. In the To field, type the names of the people that you want to add to the conversation. As you type a name, suggested names may appear. Click on a name to add this person to the conversation.



Henry Thomas, Ja... 10:34 am
good morning
Jane Moore has joined the conversation

Denise Lundberg Wednesday
You are needed in room 204.

Henry Thomas, J... Wednesday
needed in room 203
A doctor is needed in room 203.

Henry Thomas, Jane Moore
good morning

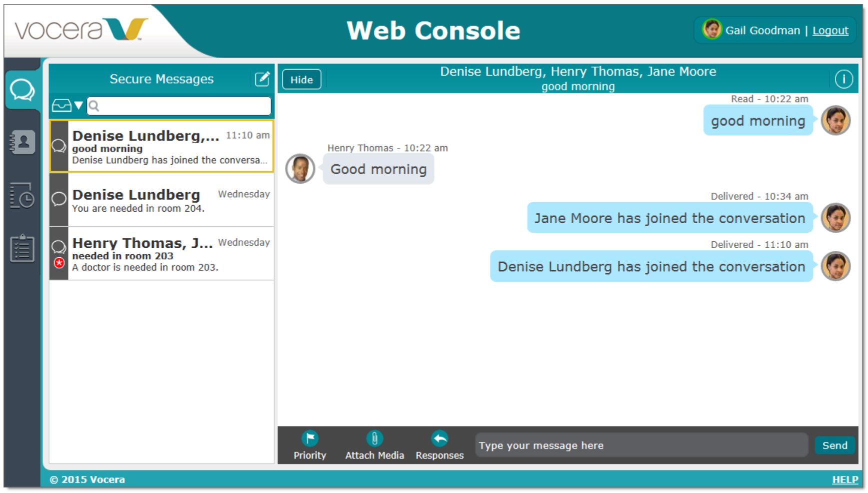
To: Henry Thomas Jane Moore De

Denise Lundberg
Psychiatrist

Subject: good morning

3. Click OK to add the new users to the message conversation.

The conversation now indicates that new people have joined.



Denise Lundberg,... 11:10 am
good morning
Denise Lundberg has joined the conversa...

Denise Lundberg Wednesday
You are needed in room 204.

Henry Thomas, J... Wednesday
needed in room 203
A doctor is needed in room 203.

Denise Lundberg, Henry Thomas, Jane Moore
good morning

Read - 10:22 am
good morning

Henry Thomas - 10:22 am
Good morning

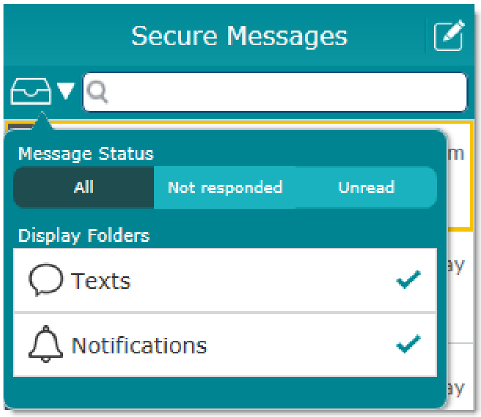
Delivered - 10:34 am
Jane Moore has joined the conversation

Delivered - 11:10 am
Denise Lundberg has joined 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 icon to display the Secure Messages Screen.
2. Click to display the filtering options.

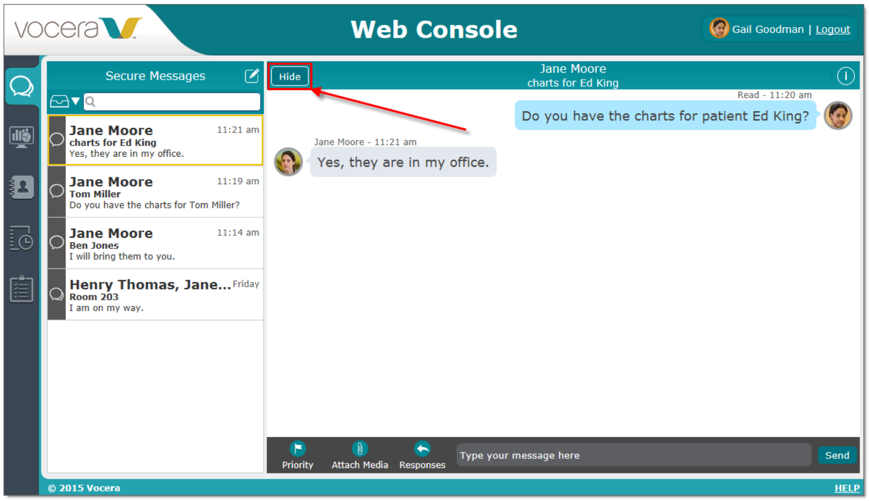


3. In the Message Status section, select whether to display all messages, messages to which you have not responded, or messages that are unread.
4. In the Display Folders section, select Texts to display text conversations, and select Notifications to display notifications. You can select either or both.
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 icon.
2. From the list of messages in the Secure Messages pane, select the message that you want to hide.
3. Click Hide.



Jane Moore 11:21 am
charts for Ed King
Yes, they are in my office.

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.

Jane Moore
charts for Ed King

Read - 11:20 am
Do you have the charts for patient Ed King?

Jane Moore - 11:21 am
Yes, they are in my office.

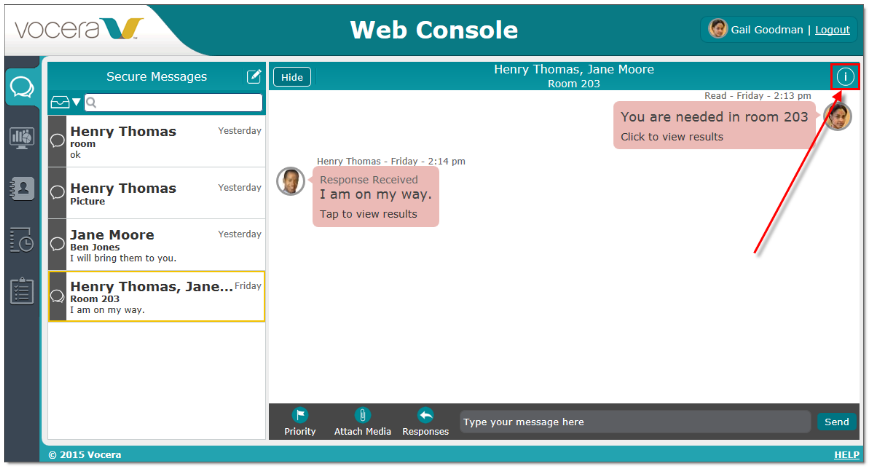
4. In the Hide Conversation dialog box, click Yes to hide the message.

Note: The message reappears if a sender or recipient that has not hidden the message continues the conversation.

Viewing Message Details

You can edit the message recipients or subject, and examine the message responses.

1. Select the Message icon.
2. From the list of messages in the Secure Messages pane, select the message for which you want to view details.
3. Click ⓘ.



Henry Thomas Yesterday
room
ok

Henry Thomas Yesterday
Picture

Jane Moore Yesterday
Ben Jones
I will bring them to you.

Henry Thomas, Jane... Friday
Room 203
I am on my way.

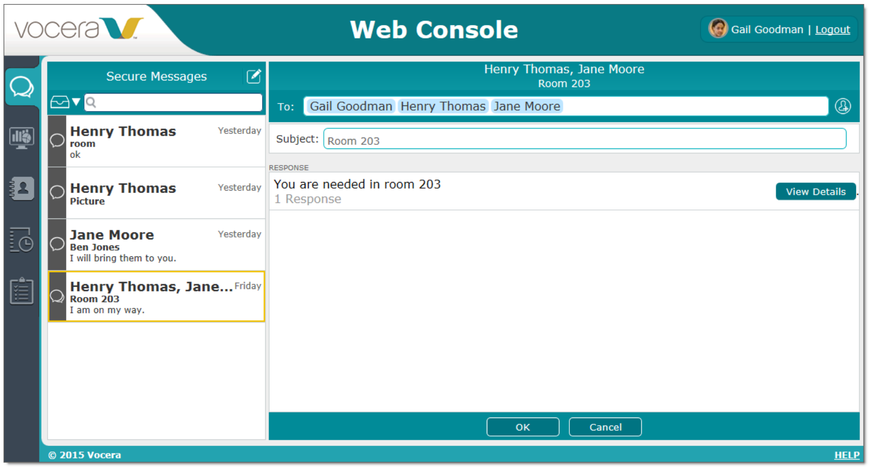
Henry Thomas, Jane Moore
Room 203

Read - Friday - 2:13 pm
You are needed in room 203
Click to view results

Henry Thomas - Friday - 2:14 pm
Response Received
I am on my way.
Tap to view results

Type your message here

The message details appear:



Henry Thomas Yesterday
room
ok

Henry Thomas Yesterday
Picture

Jane Moore Yesterday
Ben Jones
I will bring them to you.

Henry Thomas, Jane... Friday
Room 203
I am on my way.

Henry Thomas, Jane Moore
Room 203

To: Gail Goodman Henry Thomas Jane Moore

Subject: Room 203

You are needed in room 203
1 Response

For each recipient, the message status is one of the following:

Response	Description
Queued	The message is waiting to be sent.
Sent	The message has been successfully received for delivery.
Delivered	The message has been successfully delivered to the recipient's device or VMP Web Console session.
Read	The message has been read by the recipient.
Responded	The recipient has responded to the message.
Failed/Can't Deliver	The server could not send the message.
Expired	The message was not delivered within the message expiry time.

4. In the To field, select one or more users to remove from the conversation, or click 👤 to add users to the conversation.
5. Type in the Subject field to change the message subject.
6. If message responses are provided in the Response section, click View Details to display more information on the users that responded to this message.
7. Click OK to change the message, or click Cancel to cancel your changes and return to the message.

Managing User Permissions

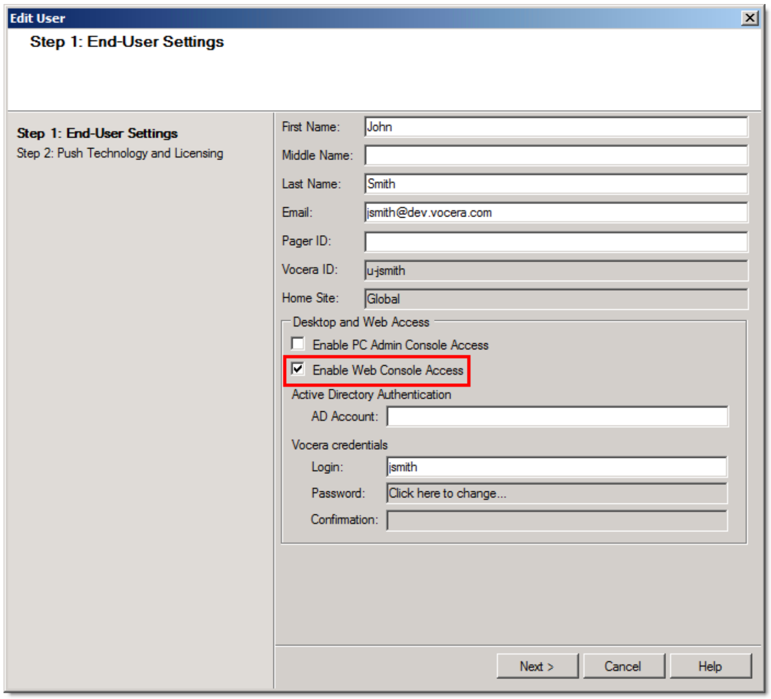
The administrator provides user permissions for access to the VMP Web Console, for creating and managing schedules, and for Alerts sent by other users.

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 (under Users).
4. Click to select Enable Web Console Access.



Step 1: End-User Settings

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

First Name: John
Middle Name:
Last Name: Smith
Email: jsmith@dev.vocera.com
Pager ID:
Vocera ID: u-jsmith
Home Site: Global

Desktop and Web Access
☐ Enable PC Admin Console Access
☑ Enable Web Console Access

Active Directory Authentication
AD Account:

Vocera credentials
Login: jsmith
Password: Click here to change...
Confirmation:

5. Provide the authentication credentials, and click Next.
6. Click Next and click Finish to save the edited account and complete the task.

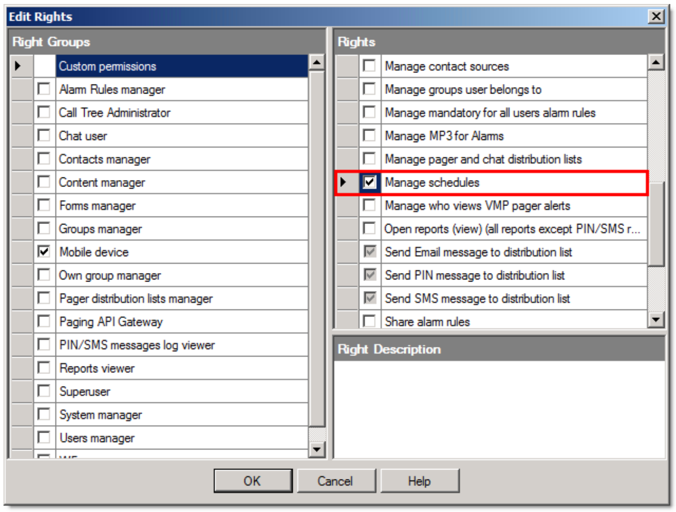
Note: You can grant VMP Web Console access to multiple users at once when importing users and contacts. See **Granting Existing Users Access to the VMP Web Console** on page 122 for more details.

Granting Users Scheduling Permissions

Users must be provided permission to create and manage schedules in the VMP Web Console. Use the following steps to assign scheduling permissions to a user.

1. Start the VMP Administrator:

   All Programs > VMP Administrator
2. Select Users & Groups > Users.
3. Click to highlight the desired user, and click User Preferences > User Rights.
4. In the Right Groups pane, select Custom permissions.
5. 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.



Right Groups:

- Custom permissions
- ☐ Alarm Rules manager
- ☐ Call Tree Administrator
- ☐ Chat user
- ☐ Contacts manager
- ☐ Content manager
- ☐ Forms manager
- ☐ Groups manager
- ☑ Mobile device
- ☐ Own group manager
- ☐ Pager distribution lists manager
- ☐ Paging API Gateway
- ☐ PIN/SMS messages log viewer
- ☐ Reports viewer
- ☐ Superuser
- ☐ System manager
- ☐ Users manager

Rights:

- ☐ Manage contact sources
- ☐ Manage groups user belongs to
- ☐ Manage mandatory for all users alarm rules
- ☐ Manage MP3 for Alarms
- ☐ Manage pager and chat distribution lists
- ☑ Manage schedules
- ☐ Manage who views VMP pager alerts
- ☐ Open reports (view) (all reports except PIN/SMS r...
- ☑ Send Email message to distribution list
- ☑ Send PIN message to distribution list
- ☑ Send SMS message to distribution list
- ☐ Share alarm rules

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 79 for more details.

6. In the Edit Rights dialog box, select the Manage all schedules checkbox to allow this user to edit all schedules that anyone has created.
7. 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.

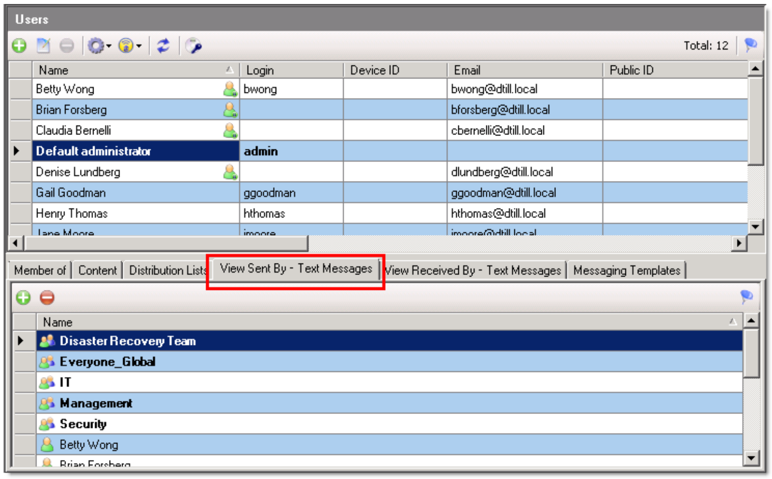
Allowing Users to View Messages

Use the following steps to allow 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

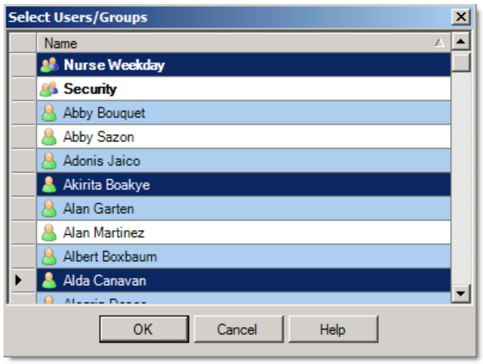
2. Select Users & Groups > Users.
3. Highlight the users to which you want to grant permission to view sent messages, and click the View Sent By - Text Messages tab at the bottom of the user list.



Name	Login	Device ID	Email	Public ID
Betty Wong	bwong		bwong@dtill.local	
Brian Forsberg			bforsberg@dtill.local	
Claudia Bernelli			cbernelli@dtill.local	
Default administrator	**admin**			
Denise Lundberg			dlundberg@dtill.local	
Gail Goodman	ggoodman		ggoodman@dtill.local	
Henry Thomas	hthomas		hthomas@dtill.local	

Name
Disaster Recovery Team
Everyone_Global
IT
Management
Security
Betty Wong

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 92 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 92.

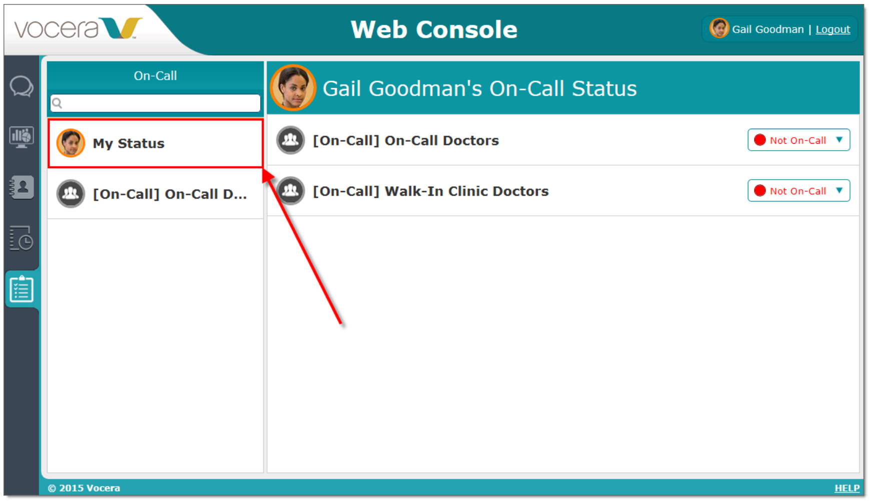
For information on how to grant users the permission to manage schedules, see **Granting Users Scheduling Permissions** on page 122.

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.

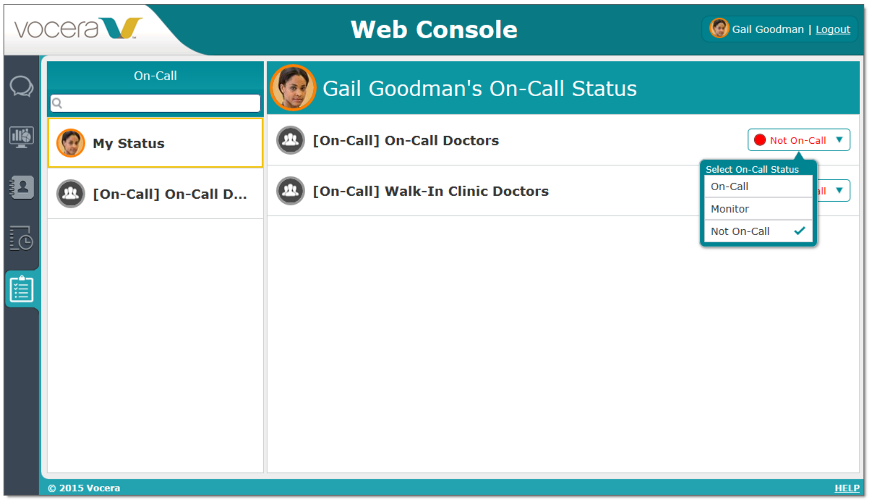
Modifying Your On-Call Status

If you are a member of an On-Call Distribution List, a published schedule can be used to determine when you are on call. This schedule automatically sets your on-call status.

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.



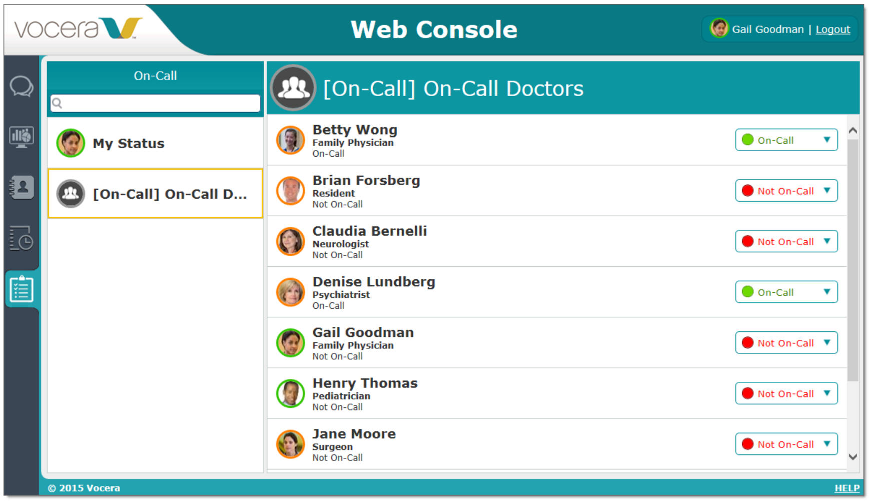
5. Change your status to one of the following:
   - On-Call - Receive messages sent to the list.
   - Monitor - Receive message sent to the list, but a response is not expected even when a message requires one.
   - Not On-Call - Do not receive messages sent to the list.

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

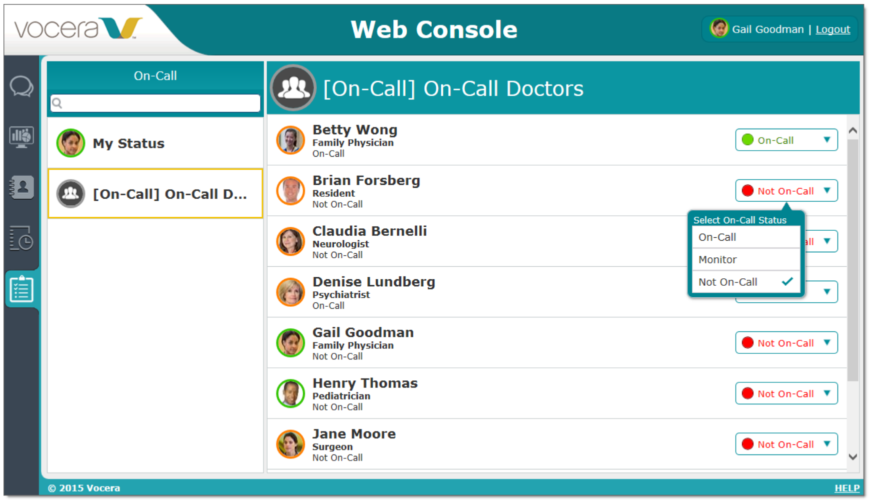
You can modify the on-call status of any user in a Distribution List.

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.



Betty Wong Family Physician On-Call	On-Call
Brian Forsberg Resident Not On-Call	Not On-Call
Claudia Bernelli Neurologist Not On-Call	Not On-Call
Denise Lundberg Psychiatrist On-Call	On-Call
Gail Goodman Family Physician Not On-Call	Not On-Call
Henry Thomas Pediatrician Not On-Call	Not On-Call
Jane Moore Surgeon Not On-Call	Not On-Call

4. For the user whose on-call status you want to change, click the user's current status. A list of options appears.



Betty Wong Family Physician On-Call	On-Call
Brian Forsberg Resident Not On-Call	Not On-Call
Claudia Bernelli Neurologist Not On-Call	
Denise Lundberg Psychiatrist On-Call	
Gail Goodman Family Physician Not On-Call	Not On-Call
Henry Thomas Pediatrician Not On-Call	Not On-Call
Jane Moore Surgeon Not On-Call	Not On-Call

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.

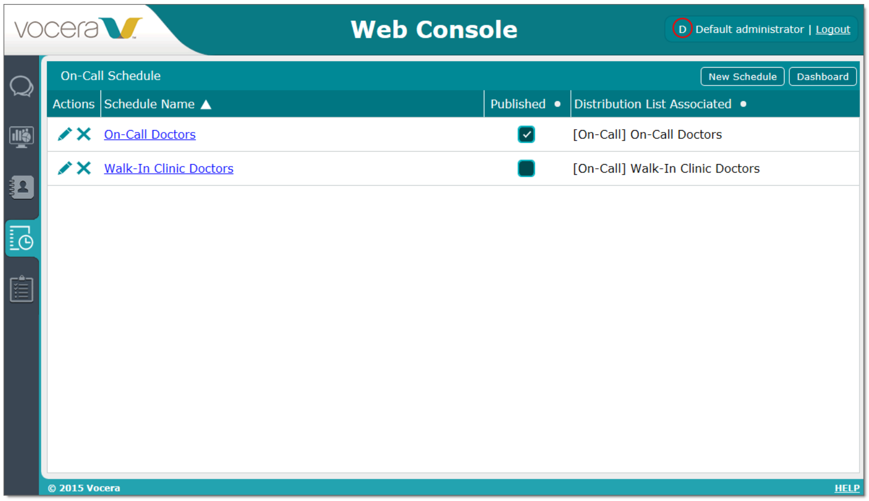
Creating On-Call Schedules

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 122.

1. Open the VMP Web Console in your Web browser.

2. Click the Schedule icon to display the list of schedules.

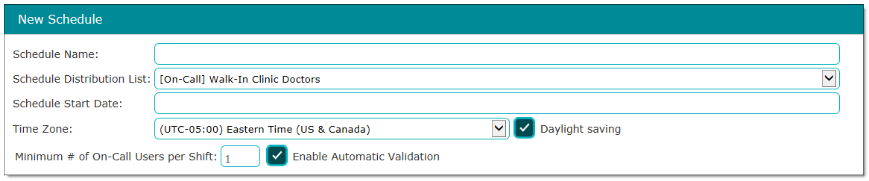


Actions	Schedule Name ▲	Published ●	Distribution List Associated ●
✎ ✕	On-Call Doctors	☑	[On-Call] On-Call Doctors
✎ ✕	Walk-In Clinic Doctors	☐	[On-Call] Walk-In Clinic Doctors

3. Click New Schedule.

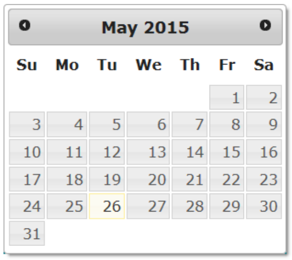
Note: If you do not have permission to create on-call schedules, the New Schedule button is not available.

4. Enter a meaningful Schedule Name.



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: 1 ☑ Enable Automatic Validation

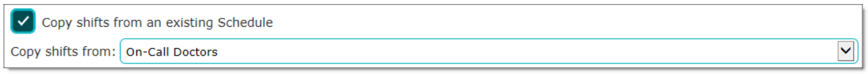
5. Use the Schedule Distribution List dropdown list to select the On-Call Distribution List (DL) for the schedule.
6. Click in the Schedule Start Date field to open the calendar picker and select the start date.



May 2015

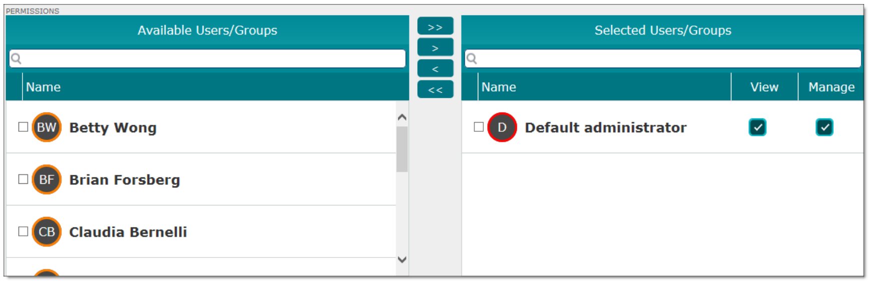
Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

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.

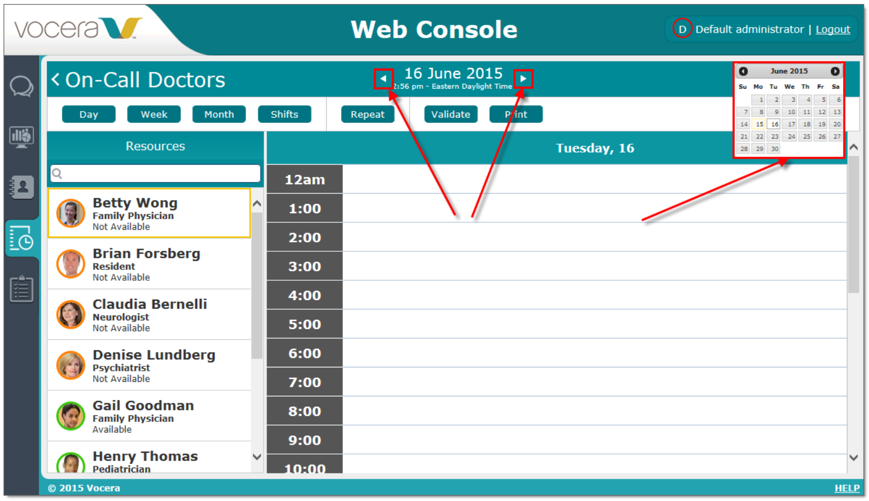


☑ Copy shifts from an existing Schedule
Copy shifts from: On-Call Doctors

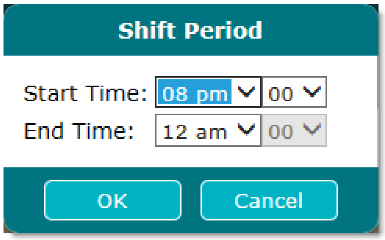
11. Use the Permissions pane to select Users/Groups with permission to access the schedule. Click to activate the checkbox next to the desired user or group and click > to select.



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.



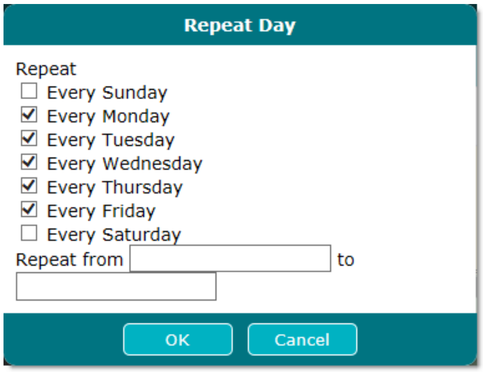
15. To assign a shift to a user, drag the user's name to the time slot that is to be the start of the shift. Use the Shift Period dialog to specify the start and end times for the shift.



Start Time: 08 pm 00
End Time: 12 am 00

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 ☐

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.

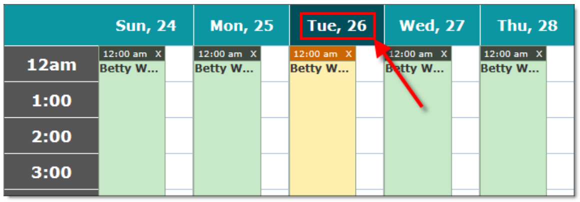
c. Click in the to field to specify the end of the date range.

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					

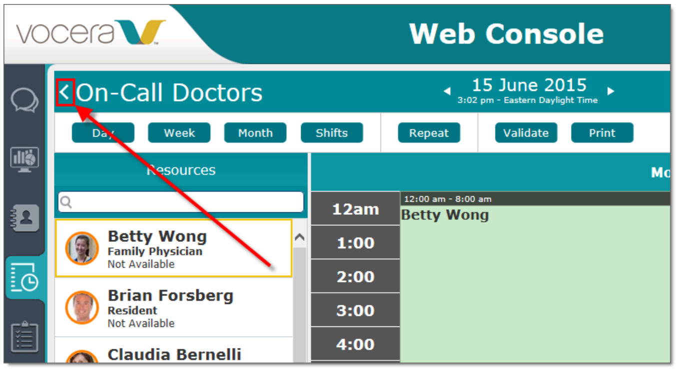
b. Click Copy.

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.



Betty Wong
Family Physician
Not Available

Brian Forsberg
Resident
Not Available

Claudia Bernelli

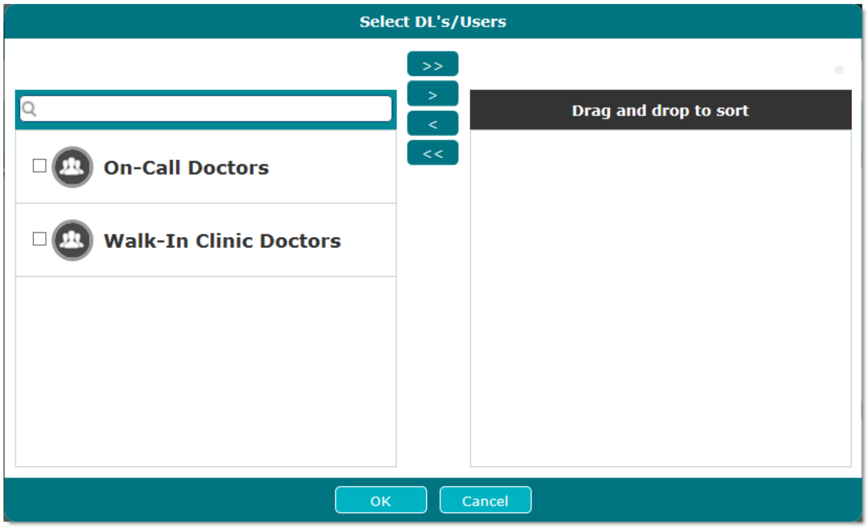
12am	12:00 am - 8:00 am Betty Wong
1:00	
2:00	
3:00	
4:00	

21. Select the Published checkbox to publish the schedule.

Viewing the Schedule Dashboard

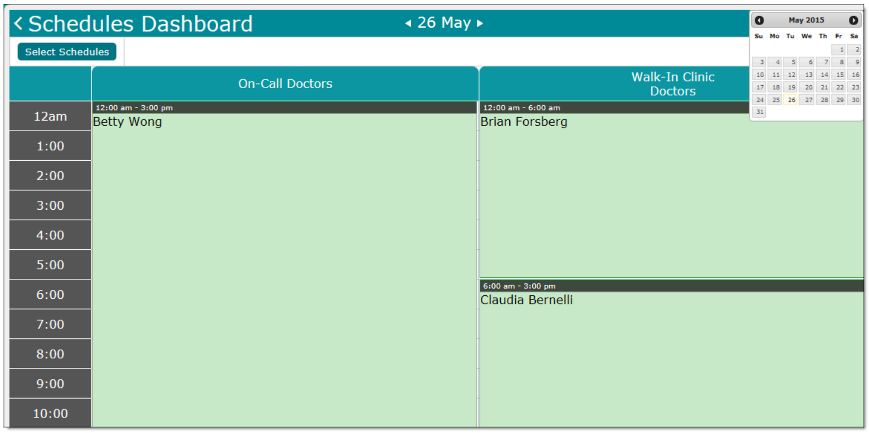
From the VMP Web Console, you can view the Schedule Dashboard, which lists any or all the schedules that you have created and who has been assigned shifts in these schedules for any specific day.

1. Open the VMP Web Console in your Web browser.
2. Click the Schedule icon.
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 <.



   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.



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 ◀ and ▶ icons to navigate to the date that you want to display.
9. Click < to return to the list of schedules.

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 the Schedule icon.
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.

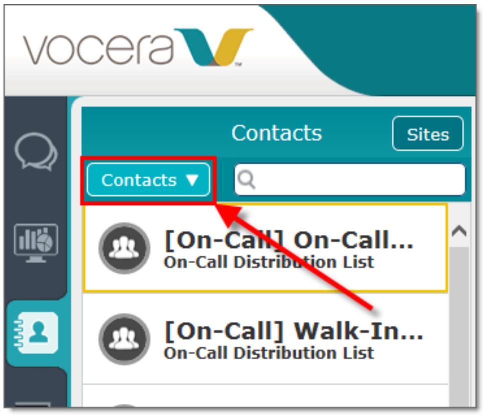
Note: Contact access is defined in the VMP Administrator. For details about defining contacts distribution lists, see **Contacts** on page 83.

Using Web Console Contacts

Use the VMP Web Console Contacts view to initiate a communication with a contact.

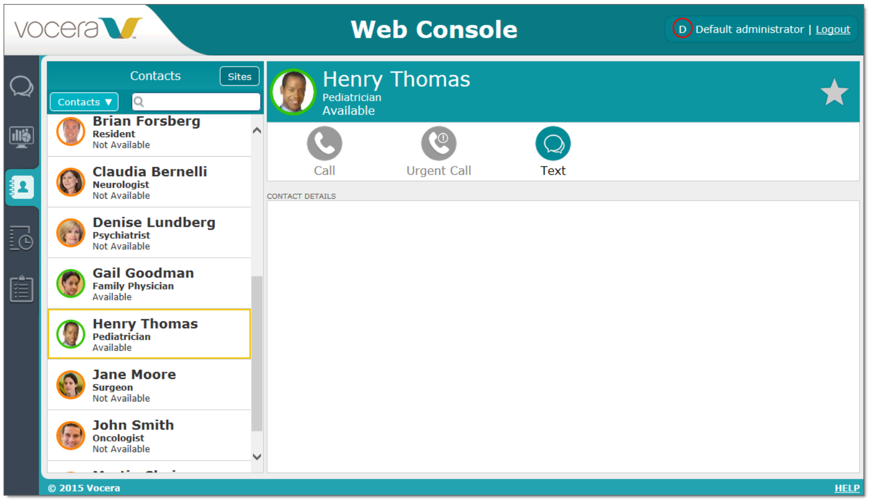
The Email option is available only for users, and is available only if the VMP Server administrator has allowed email communication. Only messages can be sent to group contacts.

1. Log on to the VMP Web Console from your Web browser.
2. Click the Contacts icon 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 132.

Select a Contact to display it:



4. 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 ‹ to return to the parent Voice Group.
5. When you have found the Contact, select Call, Urgent Call, or Text to communicate with the Contact.

Note: The Call and Urgent Call 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. Voice Groups and Distribution Lists are indicated with a 👥 icon. For each Vocera user, a photo of the user is displayed, or the user's initials if no photo is available.

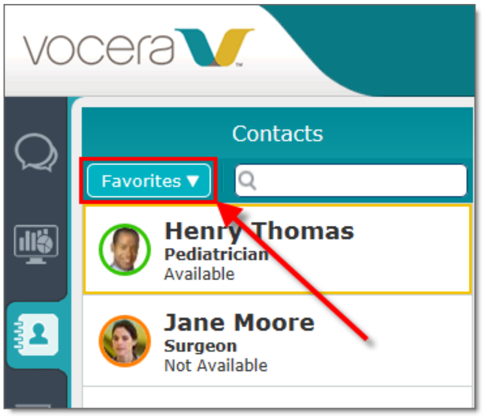
A colored ring around the user's photo or initials indicates the availability of the contact:

- Green indicates that the contact is available.
- Yellow indicates that the contact is in Do Not Disturb mode for calls, messages, or both. Details on the user's Do Not Disturb status are provided with the contact's name and title.
- Red indicates that the contact is not available.

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

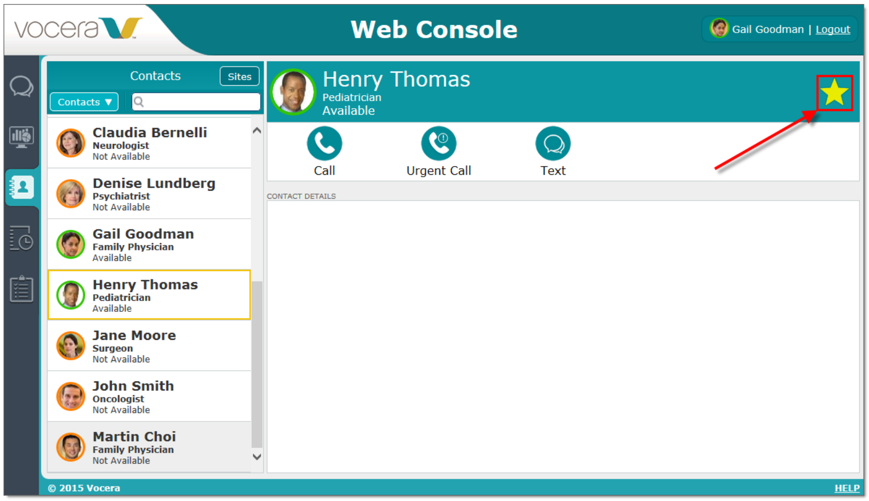
You can add a contact to the list of Favorites.

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 132 for more information on contact status.

1. Click the Contacts icon 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.

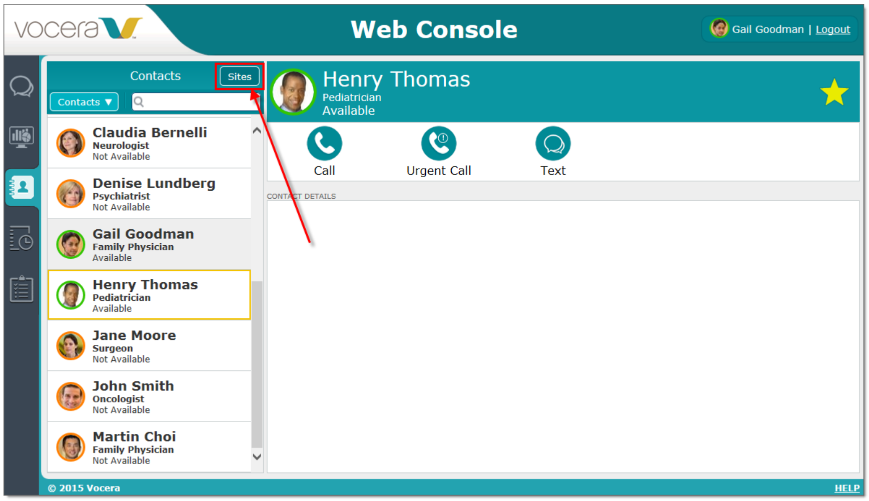


Displaying Contacts in Sites

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 26 for more information on integrating with the Vocera Voice Server.

1. Click the Contacts icon to display the Contacts view.
2. Click Sites.

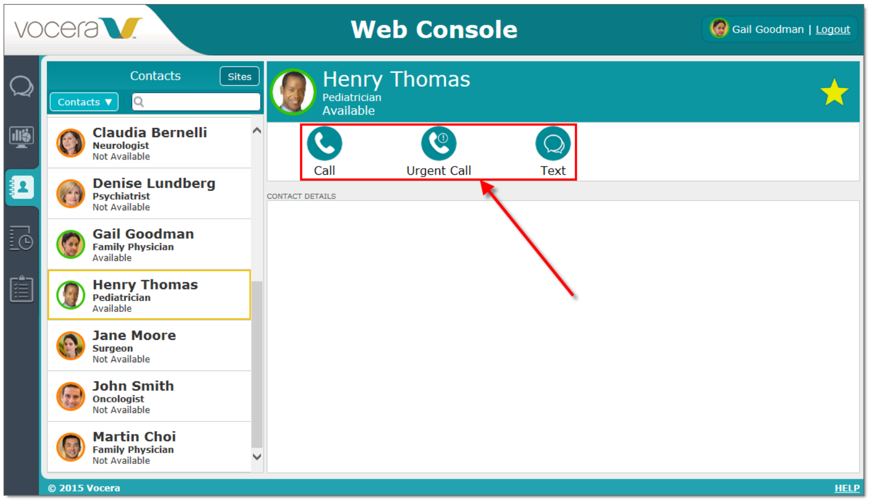


3. In the list of sites that appears, select or clear the sites to display.

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 the Contacts icon to display the Contacts view.
3. 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.



4. 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.

Appendixes

These appendixes provide additional reference information that may be useful to you.

Configuration Options Reference

The following sections list the configuration options provided for the VMP Server.

VMP Administrator Configuration Options

These are the configuration options that can be accessed from 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 37: System and Networking

Option	Description
Networking	
Vocera Messaging Server Public Host Name / IP	The IP address 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.
Email	
Enable Outgoing Email	Allow outbound email messages to be sent from the VMP Server through SMTP. These include administrative messages, Alert responses, and Open Portal reports.
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.
Security	
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.

Option	Description
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 10 for more details. You can override this setting for any individual user. For more information, see **Editing User Information** on page 78. 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 *N* most recent passwords used, where *N* 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.
User Inactivity	
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 80 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.

Table 38: 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 39: Secure Messaging

Option	Description
Enable Remind Me Later Option	Whether to display the Remind Me Later / View Later 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.

Table 40: 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 41: 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 42: Web Console

Option	Description
Disclaimer for Web Logon	
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.

Table 43: Integrations

Option	Description
Vocera Voice	
Important: If any of these values are changed, you must manually restart the VMP Server. See **Starting and Stopping the VMP Server** on page 21 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 10 for more details.

Option	Description
Port	The Vocera Voice Server port number.
Use HTTPS	Whether to use HTTPS for secure communication with the Vocera 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.
VST integration	
Enabled	Set to Yes when the VMP Server is being integrated with a Vocera Secure Texting server.
Server URL	The URL of the Vocera Secure Texting server environment. Typically, this site is accessed using HTTPS.
Server ID	The ID of the VMP Server. The Vocera Secure Texting server uses this server ID to refer to the VMP Server.
Security Token	The value sent from the VMP Server to the Vocera Secure Texting server to authenticate a connection between them.
Email	
Enable Secure Message Initiation	Enables the configuration of a user's email into the Messaging feature.
Secure Message Initiation - Incoming Mail	
Protocol	The protocol for the mailbox. This is one of POP3, IMAP4, or Exchange Web Services. Depending on the protocol selected, additional connection parameters must be specified, including POP3/IMAP/EWS Host and POP3/IMAP4/EWS Port.
Email Scan Interval	The number of seconds between scans for new incoming email.
Initiation Permitted	Indicates when Alert initiation can be triggered: • From any email address: This option allows email from any sender to initiate an Alert to the user. • From VMP users only: This option restricts Alert initiation to trigger only when the email is from another system user.
Email Username	The user name associated with the mailbox.
Email Password	The mailbox access password for the user.
Confirm Email Password	Confirm the mailbox access password for the user.
Delete Email Once Processed	Determines when email is removed from the monitored mailbox: • Immediately The email is deleted after it has been processed and converted to an Alert. • Once/Day All email is deleted after 24 hours. • Never The email is never deleted.
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 44: 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 45: 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.

VMP Enterprise Manager Configuration Options

This is a list of the configuration options that can be accessed from the VMP Enterprise Manager.

These options are organized into categories, and some categories are divided into subcategories.

To access these options, start the VMP Enterprise Manager and select Configuration ⚙.

Options marked with an asterisk * are visible only when you click Advanced Options.

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 46: VMP Enterprise Manager Configuration Options

Option	Description
Database	
Auth	
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.
Master	
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.
Services	
WDE	
NetworkInterface	The IP address of the network interface to which the server listens for requests. If this is set to `0.0.0.0`, all interfaces are available.
NetworkPort	The HTTP port number for the VMP Server.

Option	Description
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 10 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 10 for more details.
Connect to Active Directory over SSL	Whether to connect to the Active Directory server using SSL. The default is False.
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 False.
Enable automatic login using Active Directory authentication	Select True to automatically log in a Windows-authenticated user. The default is False.
Allow current logged domain user to login (display link)	Select True 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 False.

Option	Description
GCMProxy *	This value does not need to be changed.
*WCTP **	
Security code *	The security code to allow WCTP polling.
SMTP	
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.
*Network **	
*Proxy **	
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.
*Soap **	
ConnectionsLimit *	The maximum number of simultaneous SOAP connections.
Logging	
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.
Enable extended communication logging *	Enables logging of the content of HTTP requests, WCTP, and Alert emails. **Warning:** This logging information may contain Alerts and Chat messages, 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 Alerts and Chat messages.
Enable web console extended communication logging *	Enables logging of VMP Web Console data exchanges. **Warning:** This logging information will contain Alerts and Chat messages.
Enable SOAP extended communication logging *	Enables VMP SOAP interface logging.

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 47: 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)

Table 48: 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 49: 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 50: 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 51: 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

Frequently Asked Questions

This provides 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 10 .

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 Certificate** on page 71.

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/Wallace/WIC/Logs
```