stryker

Vocera XMPP Adapter Configuration Guide
Version 3.4.2

Notice

Last modified: 2023-02-24 14:56

ADP-xmpp-342-Docs build 225

Contents

Understanding a Vocera XMPP Adapter Configuration

Configure the Vocera XMPP Adapter to manage stored data, and enable communicaton with users and Vocera Platform.

Adapters send information to and receive information from Vocera Platform, as well as monitor and collect data. Each adapter is configured to allow Vocera Platform to communicate with a specific type of resource and any devices that resource may control.

For example, the Vocera XMPP Adapter manages stored data in Vocera Platform datasets to represent conversations and resources. Using these datasets, conditions and rules are configured to interact with other endpoints that are not XMPP-enabled. Vocera XMPP Adapter rules on a dataset are configured to send conversation, message, and presence information to the Vocera XMPP Adapter when this information is created by an external resource. Rules that are configured should not exceed deliverance to more than 200 users in a single conversation, as this will cause message delays.

The Vocera XMPP Adapter enables XMPP communication between Vocera users using XMPP clients by acting as the XMPP server for its configured domain. The Vocera XMPP Adapter supports communication with federated users on other XMPP domains. A self-signed security certificate generated by the Vocera XMPP Adapter must be uploaded to the federated server for federation services to function.

Only one Vocera XMPP Adapter can be active in the system. Multiple Vocera XMPP Adapter can be configured, but only one can be active at a time.

> ⚠️ **Warning:** When the site is using a mix of Cisco and XMPP devices, the **PIN Authentication Bypass for Cisco Phones** option must be enabled for a security policy implemented by the facility. See the Vocera Platform Administration Guide for more information about this security policy item.
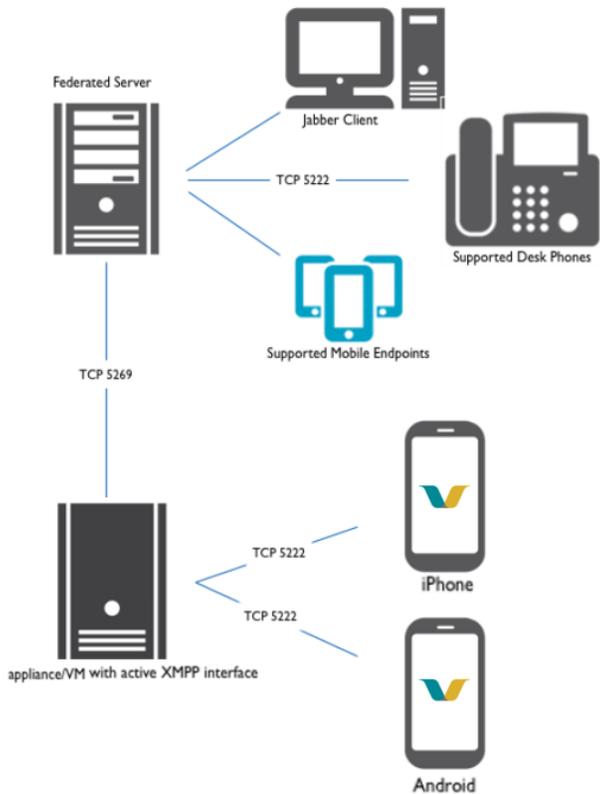
Viewing the Vocera XMPP Adapter Requirements

The minimum Vocera XMPP Adapter requirements for a Vocera Platform installation are described here.

Server

Cisco Unified Communications Manager (CUCM) version 9 or higher is optional, and not required for the Vocera XMPP Adapter to function. This CUCM version integrates the IM and Presence Services (formerly Cisco Unified Presence) in the server.

Ports

See the Vocera Platform IP Ports on page 44 tables for additional port information.

The Vocera XMPP Adapter requires two open ports: **TCP/5269** to communicate with a federated server, and **TCP/5222** to communicate with a client.

XMPP traffic on the Internet and hospital networks between the Vocera appliance and devices over port 5222 is secured by TLS. Vocera Platform provides support for use of multiple proxy servers (one per data center) in the configuration options described below.

Apple iOS

This adapter requires the port **443** for Vocera Platform to communicate with the Apple Push Notification Service (APNS).

After this communication, the APNS uses the port **5223** to communicate with a mobile device. Per Apple, port 5223 must be open in both directions for a Wifi network; see iOS Troubleshooting Push Notifications. For APNS to work from within your network, inbound and outbound TCP traffic must be enabled for **x.push.service.com** on port 5223, specifically **17.0.0.0/8:5223** must be open in both directions.

Vocera Platform then requires mobile devices to use TCP port **5222** to communicate inbound first with a proxy server, then the Vocera Appliance. If a proxy is not used, the mobile device communicates directly with the Appliance through the same port, without going through a proxy server.
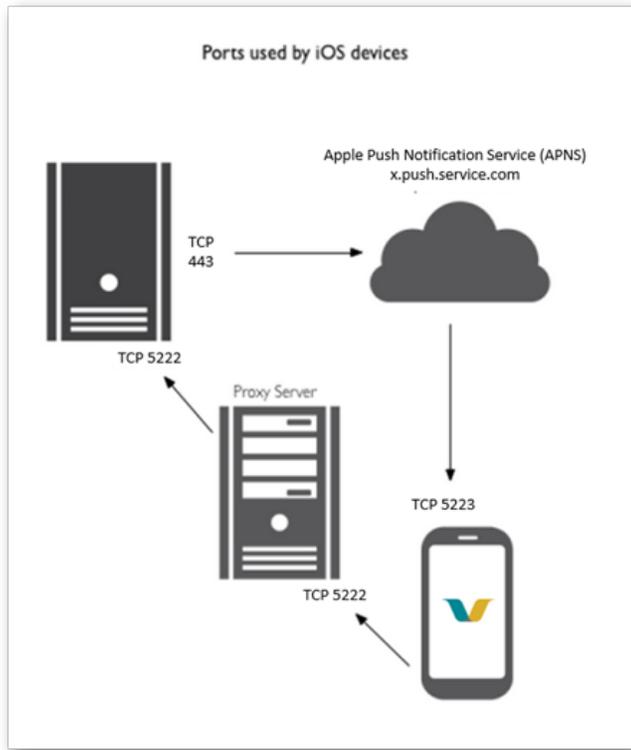
Google Android

XMPP supports Google's Firebase Cloud Messaging (FCM) service which can send remote notifications to registered devices. In addition to identifying a physical device, a token can be registered for devices that can recieve remote notifications via this Android service.

This adapter requires the port **443** for Vocera Platform to communicate with Google's Firebase Cloud Messaging (FCM) service.

After this communication, FCM uses the ports **5228, 5229, 5230** to communicate with a mobile device. Per Google, ports 5228, 5229, and 5230 must be open in both directions for a Wifi network. For FCM to work from within your network, inbound and outbound TCP traffic must be enabled for fcm.googleapis.com.

Vocera Platform then requires mobile devices to use TCP port **5222** to communicate inbound first with a proxy server, then the Vocera Appliance. If a proxy is not used, the mobile device communicates directly with the Appliance through the same port, without going through a proxy server.
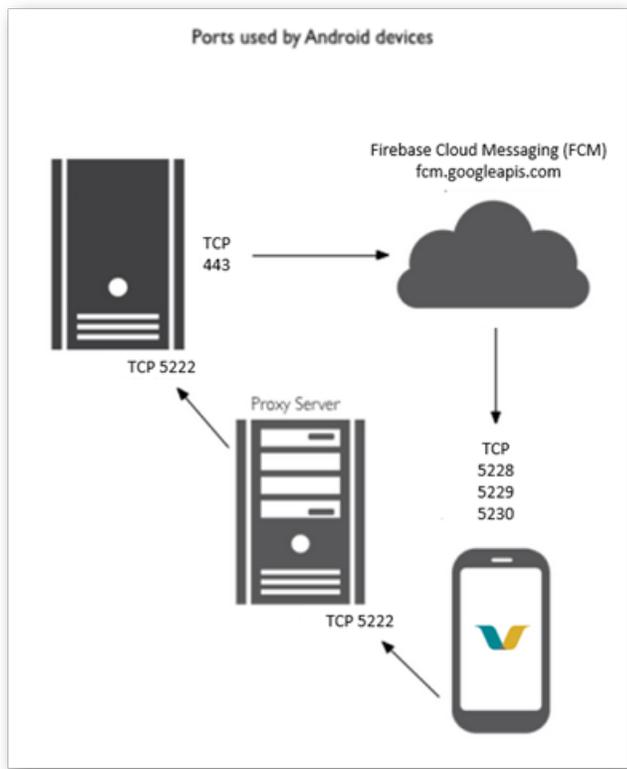
Datasets

An adapter defines a default Dataset structure in order to function. Attributes are organized by Datasets and store the information required by the adapter. Adapters use this data during the process of receiving and sending messages.

Not all adapters require Datasets to function. When an adapter does require Datasets, the system will determine if they already exist. If they do not exist, the system will create the needed Datasets.

When creating or editing an adapter, use the following information to select the appropriate datasets in the Required Datasets section.

- The ACTORS Dataset stores all actors.
- The ASSIGNMENTS Dataset stores all assignments for staff. These are used to determine who to send alerts to.
- The BEDS Dataset stores all information for beds that are registered.
- The CALL_LOG_HISTORY Dataset stores all call log history records.
- The CALL_LOG_RECEIPTS Dataset stores voicemail activity per message recipient in a conversation.
- The CONTACT_DETAILS Dataset stores all the contact details of an actor.
- The CONVERSATIONS Dataset stores all XMPP conversations.
- The CONVERSATION_HISTORY Dataset stores the history of the state progression for conversations.
- The DELIVERIES Dataset stores all message deliveries.
- The DELIVERY_HISTORY Dataset stores the progression of the status of a message through a delivery.
- The DEVICES Dataset stores all details of every device registered with Vocera. Each device to which Vocera can send a message must be listed in this dataset.
- The FACILITIES Dataset stores all facility information for a site. Represents a physical building location or campus.
- The FUNCTIONAL_ROLES Dataset stores all roles for assignments. These are used to determine the activities users can perform.

- The GROUPS Dataset stores all user groups.
- The IDENTITIES Dataset stores the user's system and interface identities.
- The LINES Dataset stores each telephone line reported by a device when it is registered.
- The LOCATIONS Dataset stores all locations. These represent a bed or group of beds to which assignments are made.
- The MESSAGES Dataset stores all individual messages generated in a conversation. This includes both standard messages as well as system messages.
- The MESSAGE_DELIVERIES Dataset stores delivery history for each message per message recipient in a conversation.
- The PATIENTS Dataset stores all patient information.
- The PLACES Dataset stores all places.
- The PRESENCE_HISTORY Dataset stores a history of all presence state changes for users.
- The PRESENCE_STATES Dataset stores all facility-defined custom presences that a user may have.
- The REGISTRATION_HISTORY Dataset stores the history of all registrations for a device.
- The ROOMS Dataset stores all information for rooms that are registered.
- The SITES Dataset stores all site information.
- The TEMPLATES Dataset stores all common messages that the user might be expected to send on a regular basis.
- The TEMPLATE_CATEGORIES Dataset stores all custom template categories. They are associated with Units.
- The UNITS Dataset stores all unit information for a site. Represents a unique care unit in a facility.
- The USERS Dataset stores all Vocera users.

ACTORS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	uid	N/A	False	N/A	True	String	Attribute that stores the unchanging uid of the actor.
Link	contact_detail	actor	False	True	N/A	One-to-many	The ACTORS Dataset is linked to the CONTACT_DETAILS Dataset, and the link order is 1:n (one actor associated to many contact_details)
Link	favorite_of	favorites	False	False	N/A	Many-to-many	The ACTORS Dataset is linked to the ACTORS Dataset, and the link order is m:n (many actors associated to many actors)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	favorites	favorite_of	False	False	N/A	Many-to-many	The ACTORS Dataset is linked to the ACTORS Dataset, and the link order is m:n (many actors associated to many actors)

ASSIGNMENTS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	assignment_id	N/A	True	N/A	N/A	String	Attribute that stores the unique identifier for the assignment.
Attribute	interface_id	N/A	True	N/A	N/A	String	Attribute that stores the identifier for the interface owning this assignment.
Attribute	level	N/A	True	N/A	N/A	String	Attribute that stores the level of the assignment.
Attribute	state	N/A	False	N/A	False	String	Attribute that stores the state of the assignment. Possible values are active, next, expired, and deleted.
Link	location	assignments	False	False	N/A	Many-to-one	The ASSIGNMENTS Dataset is linked to the LOCATIONS Dataset, and the link order is n:1 (many assignments associated to one location)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	role	assignments	False	False	N/A	Many-to-one	The ASSIGNMENTS Dataset is linked to the FUNCTIONAL_ROLES Dataset, and the link order is n:1 (many assignments associated to one functional_role)
Link	usr	assignments	False	False	N/A	Many-to-one	The ASSIGNMENTS Dataset is linked to the USERS Dataset, and the link order is n:1 (many assignments associated to one user)

BEDS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	bed_number	N/A	True	N/A	N/A	String	Attribute that stores the number of the bed.
Link	room	beds	True	False	N/A	Many-to-one	The BEDS Dataset is linked to the ROOMS Dataset, and the link order is n:1 (many beds associated to one room)
Link	locs	places	False	False	N/A	Many-to-many	The BEDS Dataset is linked to the LOCATIONS Dataset, and the link order is m:n (many beds associated to many locations)

CALL_LOG_HISTORY Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	call_log_type	N/A	False	N/A	False	String	Attribute that stores the type of the call log. Possible values are call, page, and voicemail.
Attribute	call_type	N/A	False	N/A	False	String	Attribute that stores the type of the call. Possible values are Incoming, Outgoing, Broadcast, and PanicBroadcast.
Attribute	called_group	N/A	False	N/A	False	String	Attribute that stores the uid of the called group.
Attribute	callee	N/A	False	N/A	False	String	Attribute that stores the uid of the other party.
Attribute	caller	N/A	False	N/A	False	String	Attribute that stores the uid of the calling party.
Attribute	deleted	N/A	False	N/A	False	Boolean	Attribute that stores whether or not the voice mail has been deleted.
Attribute	phone_numbe	N/A	False	N/A	False	String	Attribute that stores the phone number of the other party.
Attribute	played	N/A	False	N/A	False	Boolean	Attribute that stores whether or not the voice mail has been played.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	priority_type	N/A	False	N/A	False	String	Attribute that stores the priority for the call. Possible values include Normal, Important, Urgent, and Chat.
Attribute	result	N/A	False	N/A	False	String	Attribute that stores the result of the call.
Attribute	timestamp	N/A	False	N/A	False	Date/Time	Attribute that stores the timestamp of the call.

CALL_LOG_RECEIPTS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	voicemail_del	N/A	False	N/A	False	Date/Time	Attribute that stores timestamp at time when the voicemail was deleted.
Attribute	voicemail_pla	N/A	False	N/A	False	Date/Time	Attribute that stores timestamp at time when the voicemail was played.
Link	message	call_log_recei	True	False	N/A	Many-to-one	The CALL_LOG_RECEIPTS Dataset is linked to the MESSAGES Dataset, and the link order is n:1 (many call_log_receipts associated to one message)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	recipient	call_log_receip	True	False	N/A	Many-to-one	The CALL_LOG_RECEIPTS Dataset is linked to the IDENTITIES Dataset, and the link order is n:1 (many call_log_receipts associated to one identity)

CONTACT_DETAILS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	detail_type	N/A	True	N/A	N/A	String	Attribute that stores the type of the contact detail, such as phone or email.
Attribute	value	N/A	False	N/A	False	String	Attribute that stores the value of the contact detail.
Link	actor	contact_detail	True	False	N/A	Many-to-one	The CONTACT_DETAILS Dataset is linked to the ACTORS Dataset, and the link order is n:1 (many contact_details associated to one actor)

CONVERSATIONS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	jid1	N/A	True	N/A	N/A	String	Attribute that stores for conversations between two users, it is the alphabetically first of the users' bare JIDs. For conference rooms, it is the conference room JID.
Attribute	jid2	N/A	True	N/A	N/A	String	Attribute that stores for conversations between two users, it is the alphabetically second of the users' bare JIDs. For conference rooms, it is the string 'ROOM'.
Attribute	ttl	N/A	False	N/A	True	Integer	Attribute that stores the time-to-live (in minutes) for the conversation measured from the last message.
Attribute	activity_state	N/A	False	N/A	False	String	Attribute that stores the activity state of the conversation. Possible values are active, expired, inactive, and closed.
Attribute	topic	N/A	False	N/A	False	String	Attribute that stores the topic of the conversation.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	bookmarked_	bookmarks	False	False	N/A	Many-to-many	The CONVERSATIONS Dataset is linked to the USERS Dataset, and the link order is m:n (many conversations associated to many users)
Link	history	conversation	False	False	N/A	One-to-many	The CONVERSATIONS Dataset is linked to the CONVERSATION_HIST Dataset, and the link order is 1:n (one conversation associated to many conversation_histories
Link	members	conversations	False	False	N/A	Many-to-many	The CONVERSATIONS Dataset is linked to the USERS Dataset, and the link order is m:n (many conversations associated to many users)
Link	messages	conversation	False	False	N/A	One-to-many	The CONVERSATIONS Dataset is linked to the MESSAGES Dataset, and the link order is 1:n (one conversation associated to many messages)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	patient	conversations	False	False	N/A	Many-to-one	The CONVERSATIONS Dataset is linked to the PATIENTS Dataset, and the link order is n:1 (many conversations associated to one patient)
Link	team_member	team_convers;	False	False	N/A	Many-to-many	The CONVERSATIONS Dataset is linked to the USERS Dataset, and the link order is m:n (many conversations associated to many users)

CONVERSATION_HISTORY Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	activity_state	N/A	False	N/A	False	String	Attribute that stores the activity state the conversation has been changed to.
Link	conversation	history	False	False	N/A	Many-to-one	The CONVERSATION_HIST Dataset is linked to the CONVERSATIONS Dataset, and the link order is n:1 (many conversation_histories associated to one conversation)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	member	history	False	False	N/A	Many-to-one	The CONVERSATION_HIST Dataset is linked to the IDENTITIES Dataset, and the link order is n:1 (many conversation_histories associated to one identity)

DELIVERIES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	status	N/A	False	N/A	True	String	Attribute that stores the state of the delivered message. Possible values are Queued, Processing, Pending, Delivered, or Error.
Attribute	triggered_at	N/A	False	N/A	True	Date/Time	Attribute that stores timestamp at which the original rule was triggered.
Attribute	delivery_date	N/A	False	N/A	False	Date/Time	Attribute that stores the timestamp at which the message was delivered by the interface.
Attribute	interface_nam	N/A	False	N/A	False	String	Attribute that stores the reference name of the interface that delivered the message.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	processing_tir	N/A	False	N/A	False	Integer	Attribute that stores the duration in milliseconds from the time that the rule was triggered to when processing was completed.
Attribute	status_text	N/A	False	N/A	False	String	Attribute that stores the reason for the current status, typically an error message.
Link	history	delivery	False	False	N/A	One-to-many	The DELIVERIES Dataset is linked to the DELIVERY_HISTORY Dataset, and the link order is 1:n (one delivery associated to many delivery_histories)
Link	message	deliveries	False	False	N/A	Many-to-one	The DELIVERIES Dataset is linked to the MESSAGES Dataset, and the link order is n:1 (many deliveries associated to one message)
Link	usr	deliveries	False	False	N/A	Many-to-one	The DELIVERIES Dataset is linked to the USERS Dataset, and the link order is n:1 (many deliveries associated to one user)

DELIVERY_HISTORY Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	status	N/A	False	N/A	True	String	Attribute that stores the state of the delivered message. Possible values are Queued, Processing, Pending, Delivered, or Error.
Attribute	processing_tin	N/A	False	N/A	False	Integer	Attribute that stores the duration in milliseconds from the time that the rule was triggered to when this state was set.
Link	delivery	history	False	False	N/A	Many-to-one	The DELIVERY_HISTORY Dataset is linked to the DELIVERIES Dataset, and the link order is n:1 (many delivery_histories associated to one delivery)

DEVICES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the name that identifies the device, often based upon the MAC address of the device.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	status	N/A	False	N/A	True	String	Attribute that stores the current registration status of the device. Possible values are Registered, Disconnected, Virtual, or Unregistered.
Attribute	vendor	N/A	False	N/A	True	String	Attribute that stores the vendor of the device. For example, Cisco or XMPP.
Attribute	ip_address	N/A	False	N/A	False	String	Attribute that stores the current IP address of the device. In some cases Engage needs to keep track of the IP address of a device, such as with a Cisco phone.
Attribute	priority	N/A	False	N/A	False	String	Attribute that stores the priority level of the most recent message sent to a device. Required by the device management library, but not set by the XMPP adapter. It is used as a filter to prevent less important messages from being sent to a user currently handling a critical issue.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	token	N/A	False	N/A	False	String	Attribute that stores a special identifier needed by some devices, such as smart phones, in order to deliver a message.
Link	history	device	False	False	N/A	One-to-many	The DEVICES Dataset is linked to the REGISTRATION_HIST Dataset, and the link order is 1:n (one device associated to many registration_histories)
Link	lines	devices	False	False	N/A	One-to-many	The DEVICES Dataset is linked to the LINES Dataset, and the link order is 1:n (one device associated to many lines)
Link	usr	devices	False	False	N/A	Many-to-one	The DEVICES Dataset is linked to the USERS Dataset, and the link order is n:1 (many devices associated to one user)

FACILITIES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the unique name of the facility.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	functional_rol	facility	False	True	N/A	One-to-many	The FACILITIES Dataset is linked to the FUNCTIONAL_ROLES Dataset, and the link order is 1:n (one facility associated to many functional_roles)
Link	locations	facility	False	True	N/A	One-to-many	The FACILITIES Dataset is linked to the LOCATIONS Dataset, and the link order is 1:n (one facility associated to many locations)
Link	presence_state	facility	False	True	N/A	One-to-many	The FACILITIES Dataset is linked to the PRESENCE_STATES Dataset, and the link order is 1:n (one facility associated to many presence_states)
Link	rooms	facility	False	True	N/A	One-to-many	The FACILITIES Dataset is linked to the ROOMS Dataset, and the link order is 1:n (one facility associated to many rooms)
Link	units	facility	False	True	N/A	One-to-many	The FACILITIES Dataset is linked to the UNITS Dataset, and the link order is 1:n (one facility associated to many units)

FUNCTIONAL_ROLES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the name of the role.
Attribute	location_type	N/A	False	N/A	False	String	Attribute that stores the type of location used on an assignment for which this functional role can be associated. Possible values are single-bed and multi-bed.
Link	facility	functional_rol	True	False	N/A	Many-to-one	The FUNCTIONAL_ROLES Dataset is linked to the FACILITIES Dataset, and the link order is n:1 (many functional_roles associated to one facility)
Link	assignments	role	False	False	N/A	One-to-many	The FUNCTIONAL_ROLES Dataset is linked to the ASSIGNMENTS Dataset, and the link order is 1:n (one functional_role associated to many assignments)

GROUPS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the name of the group.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	site	groups	True	False	N/A	Many-to-one	The GROUPS Dataset is linked to the SITES Dataset, and the link order is n:1 (many groups associated to one site)
Link	units	groups	False	False	N/A	Many-to-many	The GROUPS Dataset is linked to the UNITS Dataset, and the link order is m:n (many groups associated to many units)

IDENTITIES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the name of the user's identity.
Link	call_log_receip	recipient	False	True	N/A	One-to-many	The IDENTITIES Dataset is linked to the CALL_LOG_RECEIPTS Dataset, and the link order is 1:n (one identity associated to many call_log_receipts)
Link	history	member	False	False	N/A	One-to-many	The IDENTITIES Dataset is linked to the CONVERSATION_HIST Dataset, and the link order is 1:n (one identity associated to many conversation_histories

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	message_deliv	recipient	False	True	N/A	One-to-many	The IDENTITIES Dataset is linked to the MESSAGE_DELIVERI Dataset, and the link order is 1:n (one identity associated to many message_deliveries)
Link	messages_for	recipients	False	False	N/A	Many-to-many	The IDENTITIES Dataset is linked to the MESSAGES Dataset, and the link order is m:n (many identities associated to many messages)
Link	messages_sent	from	False	False	N/A	One-to-many	The IDENTITIES Dataset is linked to the MESSAGES Dataset, and the link order is 1:n (one identity associated to many messages)
Link	usr	identities	False	False	N/A	Many-to-one	The IDENTITIES Dataset is linked to the USERS Dataset, and the link order is n:1 (many identities associated to one user)

LINES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	number	N/A	True	N/A	N/A	String	Attribute that stores number

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	device_history	line	False	False	N/A	One-to-many	The LINES Dataset is linked to the REGISTRATION_HIST Dataset, and the link order is 1:n (one line associated to many registration_histories)
Link	devices	lines	False	False	N/A	Many-to-one	The LINES Dataset is linked to the DEVICES Dataset, and the link order is n:1 (many lines associated to one device)

LOCATIONS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	location_id	N/A	True	N/A	N/A	String	Attribute that stores the unique identifier for the location.
Link	facility	locations	True	False	N/A	Many-to-one	The LOCATIONS Dataset is linked to the FACILITIES Dataset, and the link order is n:1 (many locations associated to one facility)
Link	assignments	location	False	False	N/A	One-to-many	The LOCATIONS Dataset is linked to the ASSIGNMENTS Dataset, and the link order is 1:n (one location associated to many assignments)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	places	locs	False	False	N/A	Many-to-many	The LOCATIONS Dataset is linked to the BEDS Dataset, and the link order is m:n (many locations associated to many beds)
Link	units	locations	False	False	N/A	Many-to-many	The LOCATIONS Dataset is linked to the UNITS Dataset, and the link order is m:n (many locations associated to many units)

MESSAGES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	uuid	N/A	True	N/A	N/A	String	Attribute that stores the universally unique identifier of the message.
Attribute	received_at	N/A	False	N/A	True	Date/Time	Attribute that stores the time at which the server received the message from the sending client.
Attribute	sent_at	N/A	False	N/A	True	Date/Time	Attribute that stores the timestamp at which the message was sent by the client.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	acknowledgea	N/A	False	N/A	False	String	Attribute that stores whether or not this message can be acknowledged by another message. Boolean values are 't' or 'f'.
Attribute	elements	N/A	False	N/A	False	String	Attribute that stores the raw XML of elements other than the body in the message sent.
Attribute	message	N/A	False	N/A	False	String	Attribute that stores the raw body content of the message.
Attribute	nick	N/A	False	N/A	False	String	Attribute that stores the nickname of the user that sent the message.
Attribute	state	N/A	False	N/A	False	String	Attribute that stores the state of the message. Possible values are expired, unknown, and valid.
Link	acknowledged	acknowledges	False	False	N/A	One-to-many	The MESSAGES Dataset is linked to the MESSAGES Dataset, and the link order is 1:n (one message associated to many messages)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	acknowledges	acknowledged	False	False	N/A	Many-to-one	The MESSAGES Dataset is linked to the MESSAGES Dataset, and the link order is n:1 (many messages associated to one message)
Link	call_log_recei	message	False	True	N/A	One-to-many	The MESSAGES Dataset is linked to the CALL_LOG_RECEIPTS Dataset, and the link order is 1:n (one message associated to many call_log_receipts)
Link	conversation	messages	False	False	N/A	Many-to-one	The MESSAGES Dataset is linked to the CONVERSATIONS Dataset, and the link order is n:1 (many messages associated to one conversation)
Link	deliveries	message	False	False	N/A	One-to-many	The MESSAGES Dataset is linked to the DELIVERIES Dataset, and the link order is 1:n (one message associated to many deliveries)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	from	messages_sent	False	False	N/A	Many-to-one	The MESSAGES Dataset is linked to the IDENTITIES Dataset, and the link order is n:1 (many messages associated to one identity)
Link	message_deliv	message	False	True	N/A	One-to-many	The MESSAGES Dataset is linked to the MESSAGE_DELIVERII Dataset, and the link order is 1:n (one message associated to many message_deliveries)
Link	recipients	messages_for	False	False	N/A	Many-to-many	The MESSAGES Dataset is linked to the IDENTITIES Dataset, and the link order is m:n (many messages associated to many identities)

MESSAGE_DELIVERIES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	sent_at	N/A	False	N/A	True	Date/Time	Attribute that stores the time the server sent the message to the recipient.
Attribute	acknowledged	N/A	False	N/A	False	Date/Time	Attribute that stores the time the recipient has manually acknowledged the message.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	displayed_at	N/A	False	N/A	False	Date/Time	Attribute that stores the time the message was displayed on the recipient's device.
Attribute	received_at	N/A	False	N/A	False	Date/Time	Attribute that stores the time the recipient received the message.
Link	message	message_deliv	True	False	N/A	Many-to-one	The MESSAGE_DELIVERI Dataset is linked to the MESSAGES Dataset, and the link order is n:1 (many message_deliveries associated to one message)
Link	recipient	message_deliv	True	False	N/A	Many-to-one	The MESSAGE_DELIVERI Dataset is linked to the IDENTITIES Dataset, and the link order is n:1 (many message_deliveries associated to one identity)

PATIENTS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	mrn	N/A	True	N/A	N/A	String	Attribute that stores the Medical Record Number of the patient.
Attribute	admit_date	N/A	False	N/A	False	Date/Time	Attribute that stores the admission date of the patient.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	dob	N/A	False	N/A	False	Date	Attribute that stores the date of birth of the patient.
Attribute	first_name	N/A	False	N/A	False	String	Attribute that stores the first name of the patient.
Attribute	last_name	N/A	False	N/A	False	String	Attribute that stores the last name of the patient.
Attribute	sex	N/A	False	N/A	False	String	Attribute that stores the gender of the patient.
Attribute	status	N/A	False	N/A	False	String	Attribute that stores the admission status of the patient.
Link	conversations	patient	False	False	N/A	One-to-many	The PATIENTS Dataset is linked to the CONVERSATIONS Dataset, and the link order is 1:n (one patient associated to many conversations)
Link	current_place	patient	False	False	N/A	One-to-one	The PATIENTS Dataset is linked to the PLACES Dataset, and the link order is 1:1 (one patient associated to one place)

PLACES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	patient	current_place	False	False	N/A	One-to-one	The PLACES Dataset is linked to the PATIENTS Dataset, and the link order is 1:1 (one place associated to one patient)

PRESENCE_HISTORY Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	changed_by	N/A	False	N/A	True	String	Attribute that stores indicates how the presence was changed. Possible values are user and system.
Attribute	resource	N/A	False	N/A	True	String	Attribute that stores the resource portion of the JID to which the presence history applies.
Attribute	sent_at	N/A	False	N/A	True	Date/Time	Attribute that stores the timestamp on the client device at which the message was generated.
Attribute	show	N/A	False	N/A	True	String	Attribute that stores the current presence show value for the user.
Attribute	status	N/A	False	N/A	False	String	Attribute that stores the current presence status text for the user.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	usr	presence_histo	False	False	N/A	Many-to-one	The PRESENCE_HISTORY Dataset is linked to the USERS Dataset, and the link order is n:1 (many presence_histories associated to one user)

PRESENCE_STATES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	show	N/A	True	N/A	N/A	String	Attribute that stores the presence show value to be associated with the status message. Possible values are away, chat, dnd, and xa.
Attribute	status	N/A	True	N/A	N/A	String	Attribute that stores the custom presence status message.
Attribute	duration	N/A	False	N/A	False	Integer	Attribute that stores the time (in minutes) to keep the user in the presence state.
Link	facility	presence_state	True	False	N/A	Many-to-one	The PRESENCE_STATES Dataset is linked to the FACILITIES Dataset, and the link order is n:1 (many presence_states associated to one facility)

REGISTRATION_HISTORY Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	access_point	N/A	False	N/A	False	String	Attribute that stores the access point that the device is currently connected to.
Attribute	application_ve	N/A	False	N/A	False	String	Attribute that stores the device's version of Engage.
Attribute	device_status	N/A	False	N/A	False	String	Attribute that stores the current registration status of the device.
Attribute	hardware_ver	N/A	False	N/A	False	String	Attribute that stores the device's hardware version.
Attribute	ip_address	N/A	False	N/A	False	String	Attribute that stores the device's current IP address.
Attribute	os_version	N/A	False	N/A	False	String	Attribute that stores the device's OS version.
Attribute	previous_acce	N/A	False	N/A	False	String	Attribute that stores the access point that the device was previously connected to.
Attribute	previous_ip_a	N/A	False	N/A	False	String	Attribute that stores the device's previous IP address.
Attribute	previous_wire	N/A	False	N/A	False	Integer	Attribute that stores the device's previous wireless signal strength in dBm.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	token	N/A	False	N/A	False	String	Attribute that stores some devices, such as smartphones, require a special identifier in order to receive a message. The token is used to store that special identifier.
Attribute	uuid	N/A	False	N/A	False	String	Attribute that stores the device's universally unique identifier.
Attribute	wireless_stren	N/A	False	N/A	False	Integer	Attribute that stores the device's current wireless signal strength in dBm.
Link	device	history	False	False	N/A	Many-to-one	The REGISTRATION_HIST Dataset is linked to the DEVICES Dataset, and the link order is n:1 (many registration_histories associated to one device)
Link	line	device_history	False	False	N/A	Many-to-one	The REGISTRATION_HIST Dataset is linked to the LINES Dataset, and the link order is n:1 (many registration_histories associated to one line)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	usr	device_history	False	False	N/A	Many-to-one	The REGISTRATION_HIST Dataset is linked to the USERS Dataset, and the link order is n:1 (many registration_histories associated to one user)

ROOMS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	room_number	N/A	True	N/A	N/A	String	Attribute that stores the room number.
Link	facility	rooms	True	False	N/A	Many-to-one	The ROOMS Dataset is linked to the FACILITIES Dataset, and the link order is n:1 (many rooms associated to one facility)
Link	beds	room	False	True	N/A	One-to-many	The ROOMS Dataset is linked to the BEDS Dataset, and the link order is 1:n (one room associated to many beds)
Link	unit	rooms	False	False	N/A	Many-to-one	The ROOMS Dataset is linked to the UNITS Dataset, and the link order is n:1 (many rooms associated to one unit)

SITES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the unique name for the site.
Link	groups	site	False	True	N/A	One-to-many	The SITES Dataset is linked to the GROUPS Dataset, and the link order is 1:n (one site associated to many groups)

TEMPLATES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the short name identifying the template message.
Attribute	text	N/A	False	N/A	False	String	Attribute that stores the full text of the template.
Link	template_cate	templates	False	False	N/A	Many-to-many	The TEMPLATES Dataset is linked to the TEMPLATE_CATEGOR Dataset, and the link order is m:n (many templates associated to many template_categories)
Link	users	templates	False	False	N/A	Many-to-many	The TEMPLATES Dataset is linked to the USERS Dataset, and the link order is m:n (many templates associated to many users)

TEMPLATE_CATEGORIES Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the unique name of the template category.
Link	templates	template_cate	False	False	N/A	Many-to-many	The TEMPLATE_CATEGOR Dataset is linked to the TEMPLATES Dataset, and the link order is m:n (many template_categories associated to many templates)
Link	units	template_cate	False	False	N/A	Many-to-many	The TEMPLATE_CATEGOR Dataset is linked to the UNITS Dataset, and the link order is m:n (many template_categories associated to many units)

UNITS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	name	N/A	True	N/A	N/A	String	Attribute that stores the unique name for a unit in a facility.
Link	facility	units	True	False	N/A	Many-to-one	The UNITS Dataset is linked to the FACILITIES Dataset, and the link order is n:1 (many units associated to one facility)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	groups	units	False	False	N/A	Many-to-many	The UNITS Dataset is linked to the GROUPS Dataset, and the link order is m:n (many units associated to many groups)
Link	locations	units	False	False	N/A	Many-to-many	The UNITS Dataset is linked to the LOCATIONS Dataset, and the link order is m:n (many units associated to many locations)
Link	rooms	unit	False	False	N/A	One-to-many	The UNITS Dataset is linked to the ROOMS Dataset, and the link order is 1:n (one unit associated to many rooms)
Link	template_cate	units	False	False	N/A	Many-to-many	The UNITS Dataset is linked to the TEMPLATE_CATEGO Dataset, and the link order is m:n (many units associated to many template_categories)
Link	users	unit	False	False	N/A	One-to-many	The UNITS Dataset is linked to the USERS Dataset, and the link order is 1:n (one unit associated to many users)

USERS Dataset

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	login	N/A	True	N/A	N/A	String	Attribute that stores the login name of the user.
Attribute	email	N/A	False	N/A	False	String	Attribute that stores the email address of the user.
Attribute	first_name	N/A	False	N/A	False	String	Attribute that stores the first name of the user.
Attribute	last_name	N/A	False	N/A	False	String	Attribute that stores the last name of the user.
Attribute	middle_initial	N/A	False	N/A	False	String	Attribute that stores the initials of any middle names of the user.
Attribute	photo	N/A	False	N/A	False	String	Attribute that stores the Base-64 encoded photo of the user.
Attribute	photo_type	N/A	False	N/A	False	String	Attribute that stores the content type of the photo.
Attribute	preferred_font	N/A	False	N/A	False	String	Attribute that stores the user's preferred font size. Possible values are medium or large.
Attribute	presence_show	N/A	False	N/A	False	String	Attribute that stores the current presence show value for the user.

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Attribute	presence_statu	N/A	False	N/A	False	String	Attribute that stores the current presence status message for the user.
Attribute	reference_nan	N/A	False	N/A	False	String	Attribute that stores full name of user
Attribute	title	N/A	False	N/A	False	String	Attribute that stores the title of the user.
Link	assignments	usr	False	False	N/A	One-to-many	The USERS Dataset is linked to the ASSIGNMENTS Dataset, and the link order is 1:n (one user associated to many assignments)
Link	bookmarks	bookmarked_u	False	False	N/A	Many-to-many	The USERS Dataset is linked to the CONVERSATIONS Dataset, and the link order is m:n (many users associated to many conversations)
Link	conversations	members	False	False	N/A	Many-to-many	The USERS Dataset is linked to the CONVERSATIONS Dataset, and the link order is m:n (many users associated to many conversations)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	deliveries	usr	False	False	N/A	One-to-many	The USERS Dataset is linked to the DELIVERIES Dataset, and the link order is 1:n (one user associated to many deliveries)
Link	device_history	usr	False	False	N/A	One-to-many	The USERS Dataset is linked to the REGISTRATION_HIST Dataset, and the link order is 1:n (one user associated to many registration_histories)
Link	devices	usr	False	False	N/A	One-to-many	The USERS Dataset is linked to the DEVICES Dataset, and the link order is 1:n (one user associated to many devices)
Link	identities	usr	False	False	N/A	One-to-many	The USERS Dataset is linked to the IDENTITIES Dataset, and the link order is 1:n (one user associated to many identities)
Link	presence_hist	usr	False	False	N/A	One-to-many	The USERS Dataset is linked to the PRESENCE_HISTORY Dataset, and the link order is 1:n (one user associated to many presence_histories)

Element	Name	Reverse Name	Key	Reverse Key	Required	Type	Description
Link	team_convers	team_member	False	False	N/A	Many-to-many	The USERS Dataset is linked to the CONVERSATIONS Dataset, and the link order is m:n (many users associated to many conversations)
Link	templates	users	False	False	N/A	Many-to-many	The USERS Dataset is linked to the TEMPLATES Dataset, and the link order is m:n (many users associated to many templates)
Link	unit	users	False	False	N/A	Many-to-one	The USERS Dataset is linked to the UNITS Dataset, and the link order is n:1 (many users associated to one unit)

Vocera Platform IP Ports

External and internal port information is provided in tables, including required and optional port information for platform, adapter, voice service, SIP telephony gateway, Badge, and Vina.

Users should access the application with a Fully Qualified Domain Name (FQDN). Sites using TLS should install a trusted certificate with a matching FQDN.

External Port Requirements

The following table describes the firewall requirements which should be configured in order to successfully install, update, and support the Vocera Platform and its operating system.

Port Number	Protocol	Source	Destination	Feature	Purpose
443	TCP	Vocera Platform	svc.ext-inc.com 199.180.201.227	Provisioning	Provisioning APNS certificate retrieval
22	TCP	Vocera Platform	svc.ext-inc.com 199.180.201.227	Remote Support	Remote Support

Port Number	Protocol	Source	Destination	Feature	Purpose
443	TCP	Vocera Platform	box.voceracommun address subject to change **or for legacy installations:** yum.ext-inc.com 38.99.68.43	Software Update	Repository access for installing Redhat and Vocera software updates

The following table lists optional **external** ports that may be needed depending on the configured software and desired functionality.

Port Number	Protocol	Source	Destination	Feature	Purpose
443	TCP	Vocera Platform	`api.push.apple.com17.0.0.0/8`	XMPP	Send notifications for data and calls via the Apple Push Notification Service (APNS).
5223	TCP	Vina (iOS only)	`*.push.apple.com17.0.0.0/8`	XMPP	Receive push notifications on iOS device. According to Apple, the iOS device is using Wi-Fi, port 5223 must be open outbound and inbound to the Wi-Fi.
443	TCP	Vocera Platform	Google's ASN of 15169 See Firebase firewall configuration	XMPP	Send notifications for data and calls via Firebase Cloud Messaging (FCM)
5228, 5229, 5230	TCP	Vina (Android only)	Firebase Google's ASN of 15169 See Firebase firewall configuration	XMPP	Receive push notifications on Android device
443	TCP	External browser access (all networks)	Reverse proxy # Vocera Platform Firewall pinhole # Vocera Platform Port forwarder # Vocera Platform		When workflow page access for browsers outside the network is desired using a reverse proxy in a DMZ, traffic from any address to the proxy on port 443 must be open. Using a reverse proxy also has an internal requirement for the proxy to access Vocera.
5222	TCP	Vina	Vocera Edge # Vocera Platform Firewall pinhole # Vocera Platform Port forwarder # Vocera Platform	XMPP	External XMPP traffic communicates with Vocera Platform via the Vocera Edge XMPP proxy
443	TCP	Vocera Platform	www.amion.com	Amion Adapter	Download Amion schedule updates from the Amion cloud service

Port Number	Protocol	Source	Destination	Feature	Purpose
443	TCP	Vocera Platform	`api.qgenda.com`	Qgenda Adapter	Download Qgenda schedule updates from the Qgenda cloud service

Internal Port Requirements

It is assumed that the following sources or destinations are on the internal network. If a listed item has a source or destination outside the internal network, then it must also be opened in the external firewall.

Platform Ports

Port Number	Protocol	Source	Destination	Feature	Purpose
22	TCP	Any SSH client	Vocera Platform	SSH access	Command line administration
80	TCP	Cisco Phones SpectraLink Phones	Vocera Platform	Multiple	Workflow access from mobile devices
443	TCP	Any HTTPS client	Vocera Platform	Multiple	Admin Console and workflow access via HTTPS
161	UDP	SNMP Client	Vocera Platform	SNMP	Query Vocera Platform for SNMP parameters
161	UDP	Vocera Platform	SNMP Manager	SNMP	Send SNMP traps for audit events
25	TCP	Vocera Platform	SMTP Server	SMTP	Send SMTP messages for audit events

Clustering Ports

IP packets of type 112 must be allowed for VRRP; the Virtual Router Redundancy Protocol

Port Number	Protocol	Source (Client)	Destination (Server)	Feature	Purpose
22	TCP	Master	Slave	Rsync over SSH	Filesystem replication
5432	TCP	Slave	Master	Postgres	Database replication
5433	TCP	Slave	Master	Postgres	Database replication
61616	TCP	Master Slave	Slave Master	Apache Artemis	JMS broker clustering
61617	TCP	Master Slave	Slave Master	Apache Artemis	JMS broker replication

Adapter Ports

The following port usage depends on the configured integrations.

Port Number	Protocol	Source	Destination	Feature	Purpose
9443	HTTPS	Vocera Platform	Vocera Platform	Austco	Request to register a subscription
9443	WSS	Vocera Platform	Austco	Austco	Persistent connection to receive Austco alerts
443	TCP	Multiple inbound integrations	Vocera Platform	Multiple	Inbound adapter integrations that support HTTPS; e.g., ResponderSync, Hill-Rom Clinical API, SOAP Publisher
80	TCP	Multiple inbound integrations	Vocera Platform	Multiple	Available for inbound adapter integration\ support for HTTP when HTTPS is not supported
443	TCP	Vocera Platform	Multiple outbound integrations	Multiple	Outbound adapter integrations that support HTTPS; e.g., ResponderSync, Hill-Rom Clinical API, SOAP Publisher
80	TCP	Vocera Platform	Multiple outbound integrations	Multiple	Available for outbound adapter integration\ support for HTTP when HTTPS is not supported
80	TCP	Cisco Phones SpectraLink Phones	Vocera Platform	Multiple	Workflow access from mobile devices
443	TCP	Any HTTPS client	Vocera Platform	Multiple	Admin Console and workflow access via HTTPS
5222	TCP	Vina	Vocera Platform	XMPP	Client to server XMPP traffic for all data, messaging, presence
389	TCP	Vocera Platform	LDAP Server	LDAP	Authentication and user synchronization via LDAP

Port Number	Protocol	Source	Destination	Feature	Purpose
686	TCP	Vocera Platform	LDAP Server	LDAP	Authentication and user synchronization via LDAP over SSL
1322	TCP	Vocera Platform	Unite Connectivity Manager (UCM)	Ascom	Push interactive messages to Ascom devices
5000-5004 *	TCP	UCM	Vocera Platform	Ascom	UCM responses to message delivery
5005 *	TCP	Vocera Messaging Interface (VMI) Client	Vocera Platform	VMI	Inbound VMI integrations
5007 *	TCP	Vocera Messaging Interface (VMI) Client	Vocera Platform	VMI	Inbound VMI integrations using TLS
25 *	TCP	SMTP Client	Vocera Platform	Incoming Email	Inbound SMTP messages for the Incoming Email interface
25 *	TCP	Vocera Platform	SMTP Server	Outgoing Email	Outbound SMTP messages from the Outgoing Email interface
6661-6664 **	TCP	HL7	Vocera Platform	HL7 (ADT)	Inbound HL7 ADT messages via LLP
7000,8000-8010 **	TCP	HL7	Vocera Platform	HL7 (Alarms)	Inbound HL7 Philips, Capsule or IHE compliant Alarm messages via LLP
12000	TCP	Navicare Server	Vocera Platform	Navicare	Inbound Hill-Rom Navicare messages
2000 *	UDP	Carescape Network	Vocera Platform	Carescape	Time synchronization
70001	UDP	Carescape Network	Vocera Platform	Carescape	Device discovery
7001 *	UDP	Carescape Network	Vocera Platform	Carescape	Monitor Alarm Messages
5050 *		EarlySense Gateway	Vocera Platform		

Voice Service Ports

Port Number	Protocol	Source	Destination/Feature
5002	UDP	Badge	Vocera Server Signaling
5001	TCP	Vocera SIP Telephony Gateway	Vocera Server Signaling
5400	UDP	Badge/Badge Property Editor	Updater Signaling
5100	UDP	Badge	Vocera Server Audio
7200-7263	UDP	Badge	Vocera Server Audio Recording
7892 - 9100 [1]	UDP	Vocera Server	Badge/VSTG Audio
3306	TCP	MySQL Signaling	(Listening)
5251	TCP	Vocera Server Cluster Signaling	(Listening)
5555-5556	UDP	Badge	Vconfig (Vch) Signaling during Discovery
5555-5556	TCP	Badge	Vconfig (Vch) Signaling during Discovery
7023	TCP	Nuance Watcher Telnet Client	(Listening)
7890	UDP	Nuance Watcher	(Listening)
27000	TCP	Nuance License Manager	(Listening)
5059, 5058	TCP	Nuance Speech Server (allows UDP connections)	(Listening)
8200	TCP	Nuance Recognition Server	(Listening)
32768-60999	TCP	Vina (iOS only)	Signaling Gateway
32768-60999	UDP	Vina (Android only)	Signaling Gateway

SIP Telephony Gateway Ports

This section provides information on ports supported for Vocera SIP Telephony Gateway (VSTG).

Note: Support for VSTG is added in Vocera Platform version 6.1.0 and later releases.

---

[1] Only **even**-numbered ports are used. The range is configurable in \vocera\nuance\SpeechServer \config\NSSserver.cfg.

Port Number	Protocol	Source	Destination/Feature	Direction
5060	UDP	IP PBX	Vocera SIP Telephony Gateway Signaling	Bidirectional
5300-5555[2]	UDP	Vocera Platform	Vocera SIP Telephony Gateway Audio	Outbound
9200 - 9399 4000 - 4049	UDP	IP PBX	Vocera SIP Telephony Gateway Audio (RTP/RTCP)	Outbound
Any free port	UDP	Vocera Platform	Vocera SIP Telephony Gateway Signaling	Outbound

Badge Ports

Port Number	Protocol	Source	Destination/Feature	Direction
5002	UDP	Badge	Server Signaling	Bidirectional
5200	UDP	Vocera SIP Telephony Gateway	Badge Audio	Outbound
5400	UDP	Badge	Updater	Outbound
5555-5556	UDP	Badge	Updater Signaling	Bidirectional
5555-5556	UDP	Badge	Vconfig (Vch) Signaling during Discovery	Bidirectional
5555-5556	TCP	Badge	Vconfig (Vch) Signaling during Discovery	Bidirectional

---

[2] Only **even**-numbered ports are used. The range is configurable in \vocera\nuance\SpeechServer \config\NSSserver.cfg.

Vina Ports

Port Number	Protocol	Source	Destination	Feature	Purpose
5222	TCP	Vina	Vocera Platform Vocera Edge Firewall pinhole Port forwarding	XMPP	Client to server XMPP traffic for all data, messaging, presence. Communication with Edge proxy or other customer configured port 5222 access will off-premise.
32768-60999	TCP	Vina (iOS only)	Vocera Platform	Signaling Gateway	Call signaling and notifications
32768-60999	UDP	Vina (Android only)	Vocera Platform	Signaling Gateway	Call signaling and notifications
5800-5899	UDP	Vina	Vina	RTP	Client to client VoIP

Vocera Analytics Ports

This section provides information on ports supported for Vocera Analytics.

Port Number	Protocol	Source	Destination	Direction
9445	TCP	Voice Server (Remote Agent)	(Listening)	Inbound
4040	TCP	VA Server	Spark UI	Inbound
7778	TCP	VA Server (VMP Flume agent)	Spark	Bidirectional
7779	TCP	VA Server (Engage Flume agent)	Spark	Bidirectional
7780	TCP	Voice Server (VS Flume Agent)	Spark	Bidirectional
8443 (default) or user defined	TCP	VA Server (Reporting service)	(Listening)	Inbound
3306	TCP	Maria DB Signaling	(Listening)	Inbound

Legend

* These are the default values. The installer can choose a different port when configuring the adapter.

** These are the default values. The installer can choose a different port **or add more ports** when configuring the adapter.

Configuring a Vocera XMPP Adapter

Description of the settings that enable direct communication between the Vocera XMPP Adapter and the Vocera Platform.

Select an empty field and begin typing, or select an existing value and type over it. To keep an existing value, do not edit that field.

1. Access the Vocera Platform Web Console and navigate to the adapters.

   See Navigating the Vocera Platform Adapters on page 96 for instructions.

2. Select **New Adapter** in the Action menu, or select an adapter you wish to configure and then select **Edit**, to display the configuration fields. The configuration fields are the same for new and existing adapters.

3. Navigate to the New Adapter option, or navigate to an existing adapter to edit. See Creating a New Adapter on page 99 and Editing an Adapter on page 98 for instruction as needed.

   The configuration fields are the same for new and existing adapters.

4. Complete the configuration fields as described in the table, for new or existing adapters. This table describes a portion of the fields provided in the configuration dialog.
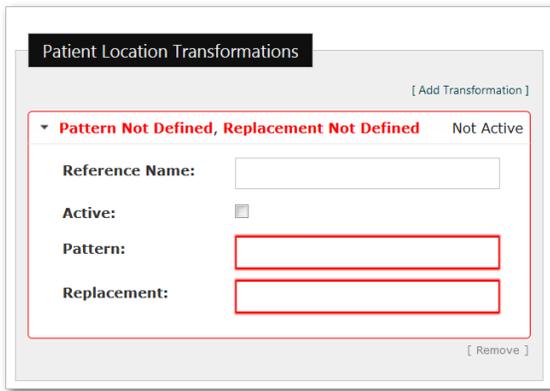

Configuration Field	Description
Component Name	Click the Component Name field to display a list of the systems and devices that the Vocera Platform currently supports. Select the name of the adapter to create.
Reference Name	Enter a short descriptive name in the Reference Name field to uniquely identify an adapter instance. It may demonstrate the adapter function or other information; for example, Production adapter may differentiate a live adapter from a development or "sandbox" adapter.

Configuration Field	Description
Enabled	Select the Enabled checkbox to allow the Vocera Platform to use the new adapter. The Vocera Platform ignores the adapter if this option is disabled.
Required Datasets	If more than one dataset exists that meets the adapter's requirements, select the appropriate datasets for the new adapter to function correctly. The system searches for the datasets that meet the adapters requirements. If the datasets already exist, the system will use them. If the datasets do not exist, the system will create them automatically. Select Create in the drop-down menu to create a new dataset to meet the organization's requirements, if needed. **Note:** If Rules in a dataset are configured in a way that multiple rules fire for the same alert at the same time, some messages may not be delivered.

5. Complete the **Main Adapter Settings** configuration fields as described in the table, for new or existing adapters. This table describes a portion of the fields provided in the configuration dialog.

Main Adapter Settings Configuration Field	Description
Chat Domain	Enter the domain name for which the XMPP server will respond, such as facility.net or company.com. This should be a unique name that identifies the instance of the Vocera XMPP Adapter. Set this domain name in the DNS to allow XMPP clients to locate the service. **Warning:** The DNS must be configured to have the same domain, for example "vocera.myhospital.com", points to the Vocera Platform appliance (internally) and to Edge (externally). Failure to do so will prohibit the Vocera Platform appliance from functioning properly.
Vocera Help Link	Enter a help link used by the XMPP mobile client to direct a user to a webpage that can be used to offer limited support.

Main Adapter Settings Configuration Field	Description
Mobile Session Timeout	Select a time duration of **Off**, **13 hours**, or **7 days** from the drop-down menu. This setting defines the period of time that the mobile client will allow the current user to stay logged in after the mobile application goes into the background. Once the selected threshold is passed, the current user is automatically logged out of Vocera Platform. Mobile Session Timeout will never expire when it is set to Off, and the user will remain logged in indefinitely. Otherwise, select 13 hours or 7 days as the timeout value.
Desktop Session Timeout	Select a time duration of one of the listed options in minutes, hours, or days from the drop-down menu. This setting defines the period of time that the desktop client will allow the current user to stay logged in after the last activity in the mobile application. Once the selected threshold is passed, the current user is automatically logged out of Vocera Platform. Desktop Session Timeout will never expire when it is set to Off, and the user will remain logged in indefinitely.
Offline Message Timeout	Select a time duration from the drop-down menu. This setting defines the period of time that the Vocera client will store messages in memory for offline users. Once the selected threshold is passed, the messages will no longer be stored. Selecting **Default** will use the best practice timeout for the current adapter release version. For example, the best practice default value is 7 days.
Disable Acknowledgments	Select this option to disable message acknowledgment support. This checkbox does not actually disable storing Acknowledgeable Messages or their responses; this checkbox only prevents detection of the feature.

6. Complete the **Roster** configuration fields as described in the table, for new or existing adapters. This table describes a portion of the fields provided in the configuration dialog.

Roster Configuration Field	Description
Multiple Facility	Select this checkbox for installations that service more than one facility, where unit names may be duplicated. When the Vocera XMPP Adapter is configured for multiple facilities, the unit names in the roster will have the facility name prefixed to the unit. For example, an installation can differentiate two ICUs in the device roster by displaying the facility name; Central ICU and North ICU.
Prefix for Assignment Level 1	Enter the value to be added as a prefix to the role name for assignments with a level value of "1" when an assignment for the same location and role exists with level "2". If the value is not set (due to an older configuration), the value 'Primary' is used.

Roster Configuration Field	Description
Prefix for Assignment Level 2	Enter the value to be added as a prefix to the role name for assignments with a level value of "2" when an assignment for the same location and role exists with level "1". If the value is not set (due to an older configuration), the value 'Backup' is used.

7. Complete the **Phone Number Transformations** configuration fields as described in the table, for new or existing adapters. This table describes a portion of the fields provided in the configuration dialog.

   Phone number transformations are site specific settings needed by Vocera Vina clients. These settings are transparent to the Vocera XMPP Adapter and are passed to Vocera Vina clients when client settings are retrieved. These allow phone numbers dialed by Vocera Vina clients to be modified so the call can be completed depending on the client's dialing configuration (VOIP vs Cellular).

   When a Vocera Vina user dials a phone number and the client is configured to dial using Cellular, the Vocera Vina client will scan the list of phone number transformations and apply the first one which matches the pattern. When the number matches the patten, the mask associated with the matched patten is applied to the number. The call is then routed with the new number. Each phone number transformation requires a mask, pattern, and an active flag. The transformation can also take an optional reference name.

Phone Number Transformations Configuration Field	Description
Reference Name	Enter an identifier for the phone number transformation entry. This field is optional.
Active	Select the checkbox to flag the transformation as active in the system.
Pattern	Enter the pattern for the phone number to match. In a matching pattern, X will match any digit, and the number of digits must match the number of digits in the phone number. Spaces and these characters are ignored: **) - , . (** Patterns are applied when Cellular dialing is selected in Vocera Vina, to support dialing an internal number from the Cellular network. Patterns are also applied when Jabber or VOIP dialing is selected in Vocera Vina and the dialed number is 10 digits or longer, to support dialing an external number with a prefix from the internal network.
Mask	Enter the mask to apply to the phone number in the transformation.

8. Complete the **Patient Details** configuration fields as described in the table, for new or existing adapters. This table describes a portion of the fields provided in the configuration dialog.

The Vocera XMPP Adapter can provide patient details in addition to the default information and any alert context. For example, these patient details can also be used when linking a patient to a conversation.

The default patient attributes include first and last name, date of birth, sex, and facility admit date. The Vocera XMPP Adapter can be configured to query the database for additional patient attributes when the following Patient Details fields are configured.

Once created, the patient details are ordered by default attributes first, and followed by the sortable items configured as described here.

Patient Details Configuration Field	Description
Label	Enter a unique label for the value to be added to the patient details. This field is required. For example, enter 'airstripone.room' when the room that the patient is admitted to should be included in the additional patient details.
Attribute Path	Enter the attribute path of the value to be added to the patient details. This field is required. For example, enter the 'bed.room.room_number' attribute path in this field to add the patient's room to the details.
Hidden	Check the Hidden checkbox to configure the adapter to not display the patient detail in the client. When the patient detail is used in a third party integration, the customer may prefer not to display the specified data in the client. When this checkbox is selected, the label in the upper right corner of the Patient Details window changes from 'Not Hidden' to 'Hidden'.

9. Complete the **Patient Locaton Transformation** configuration fields as described in the table, for new or existing adapters. This table describes a portion of the fields provided in the configuration dialog.

   Patient Location Transformations are an ordered list of regex pattern and replacement pairs. These transformations are applied to a patient location with the intent of shortening the location string while preserving readability.

   The first active transformation with a regex matching the location is applied to transform the location. The transformed location is then used for the location to display within the patient context (e.g., in patient-linked conversations, alerts, and roster).

Patient Locaton Transformation Configuration Field	Description
Reference Name	Enter the identifier for the patient location transformation entry.
Active	Select the checkbox to flag the transformation as active in the system.
Pattern	Enter the regex pattern used to match a patient's location, such as **ICU(.*)**.
Replacement	Enter the replacement to be applied to the location in the transformation. Capture groups can be referenced via the dollar sign, such as **ICU$1**. Note that the replacement is only done once on the location.

10. Complete the **Custom Parameters** configuration fields as described in the table, for new or existing adapters. This table describes a portion of the fields provided in the configuration dialog.

Custom parameters allow the facility to define settings to be added to an alert. These settings are transparent to the Vocera XMPP Adapter, and are simply passed to the Vocera Vina application when client settings are retrieved.

Use the custom parameter configuration to create site-specific settings. The parameter name identifies the custom setting, and the defined value is added to the alert. For example, a custom parameter named "airstripone.siteid" could add the value "2030" to an alert.

To override a custom parameter, enable an alert rule using the same name.

Custom Parameters Configuration Field	Description
Parameter	Enter the name of the custom parameter to be added to the alert.
Value	Enter the value of the custom parameter to be added to the alert.

11. Select one of the available options to exit the adapter configuration page. See Saving an Adapter on page 100 for details.

Using the XMPP Certificate Manager

A security certificate is required to create an encrypted, authenticated channel between the XMPP server and clients, as well as federated servers and the Vocera XMPP Adapter on the appliance.

The Vocera XMPP Adapter and Vocera Vina clients require Transport Layer Security (TLS) protocol encryption for the XMPP stream.

A security certificate is required to create an encrypted, authenticated channel between the XMPP server and clients, as well as federated servers and the Vocera XMPP Adapter on the appliance. Additionally, if the customer is in the iOS Developer Enterprise Program and will re-sign and re-distribute the Vocera Vina application, they may want to provide their own APNs certificate.

To support TLS, the Vocera XMPP Adapter has the ability to generate a self-signed certificate, as well as generate a Certificate Signing Request (CSR). A CSR is submitted to a Certificate Authority (CA) in order to obtain a certificate signed by the CA (a security certificate). Each configuration for the Vocera XMPP Adapter will maintain its own TLS certificate, as well as its own temporary certificate for a CSR in progress.

To use a signed security certificate, customers will generate a CSR from the XMPP Certificate Manager, send the CSR to a Certificate Authority (such as VeriSign) to receive a signed certificate in return, and upload the signed certificate to the Vocera XMPP Adapter using the XMPP Certificate Manager.

Upon startup, the Vocera XMPP Adapter immediately checks the expiration date of the current certificate. For all XMPP configurations which use a certificate that was signed by a Certificate Authority, the Vocera XMPP Adapter also registers a service which will check the expiration date on the signed certificate. If the service determines that a certificate expiration date is within one month of the current date, notification is sent as an audit event. When a self-signed certificate expires, the Vocera XMPP Adapter replaces the expired certificate with a newly generated self-signed certificate. CA signed certificates are not automatically replaced.

Log into the Vocera Platform Web Console to access the **XMPP Certificate Manager** in the **Additional XMPP Adapter Actions** panel as shown below. The Certificate Manager provides the ability to:

- View certificate information for this configuration.
- Download the certificate for this configuration.
- Upload a new certificate for this configuration.
- Delete the certificate for this configuration.
- Generate and download a CSR.
- Upload an Apple APNs certificate.

Federating the Servers

A federated server is configured to receive requests, and distribute these requests to the data sources.

Each Vocera XMPP Adapter configuration will maintain its own TLS certificate, as well as its own temporary certificate for a CSR in progress.

First, set the **domain name** for the XMPP server in the Vocera XMPP Adapter configuration field, and start the adapter on the appliance.

In the Vocera Platform Web Console, navigate to the Vocera XMPP Adapter and view the **Additional Actions** options in the sidebar help section. The following operations can be performed by an administrator from the **XMPP Certificate Manager**.

Download the Current TLS Certificate

Click **Download Certificate** to download the server's current TLS certificate. A servlet request is made to extract the certificate and return it as a file to be downloaded by the web browser. The certificate is encoded in PEM format.

Once downloaded, navigate to the federated server and install the certificate to allow the server to authenticate the certificate and enable presence and federation services. See **Replace an Existing XMPP Certificate on the Cisco Unified Communications Manager IM and Presence Server** in Configuring the Federated Server to Work with Vocera Platform on page 88.
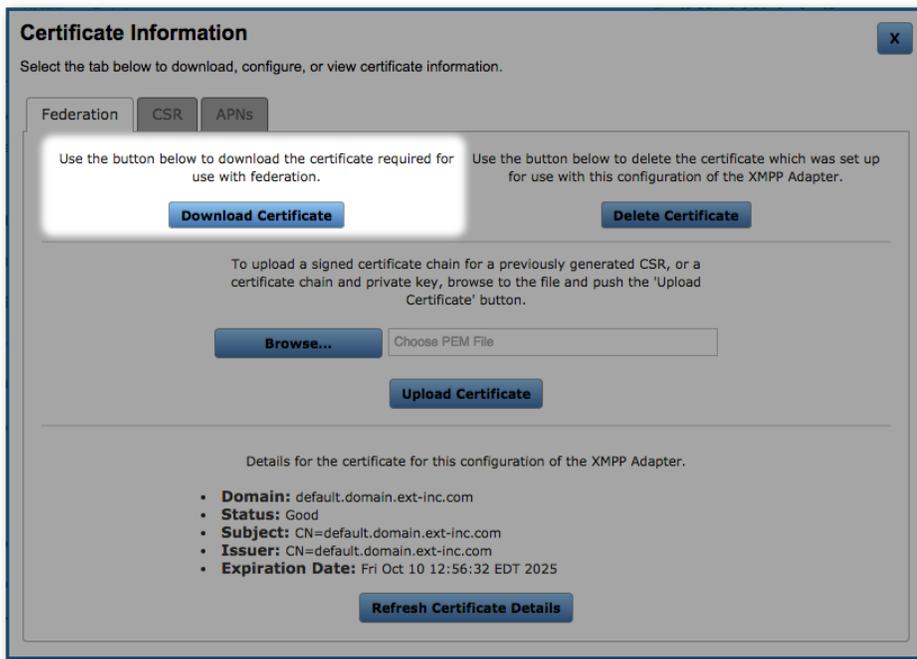
Delete the Server Certificate

Click **Delete Certificate** to delete the server certificate. A servlet request is made to delete the TLS certificate from the KeyStore generated by the adapter. Once the certificate is deleted, the Vocera XMPP Adapter will generate a self-signed certificate.
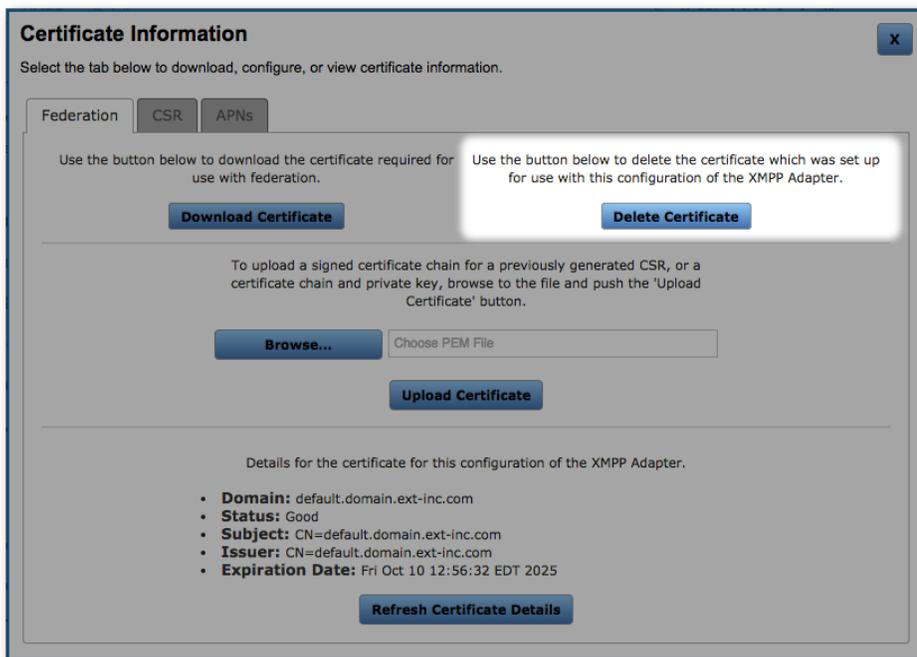
Upload the TLS Certificate

Browse to locate the TLS certificate associated with the currently loaded CSR and click **Upload Certificate** to upload the file. A servlet request is made to upload the certificate into the KeyStore with the private key used to sign the CSR. Alternatively, the administrator may upload a PEM file that includes the private key for the certificate being uploaded. In either case, the uploaded file must:

- Be a PEM file
- Contain the TLS certificate first
- Contain any intermediate certificates (in order) after the TLS certificate
- Optionally contain a private key last

Once clicked, a status at the bottom of the page indicates the success or failure of this operation. Existing mobile SSL connections to the XMPP server continue to use the TLS credentials of the previous certificate. Mobile SSL connections made after the certificate upload will use the new certificate when negotiating TLS.
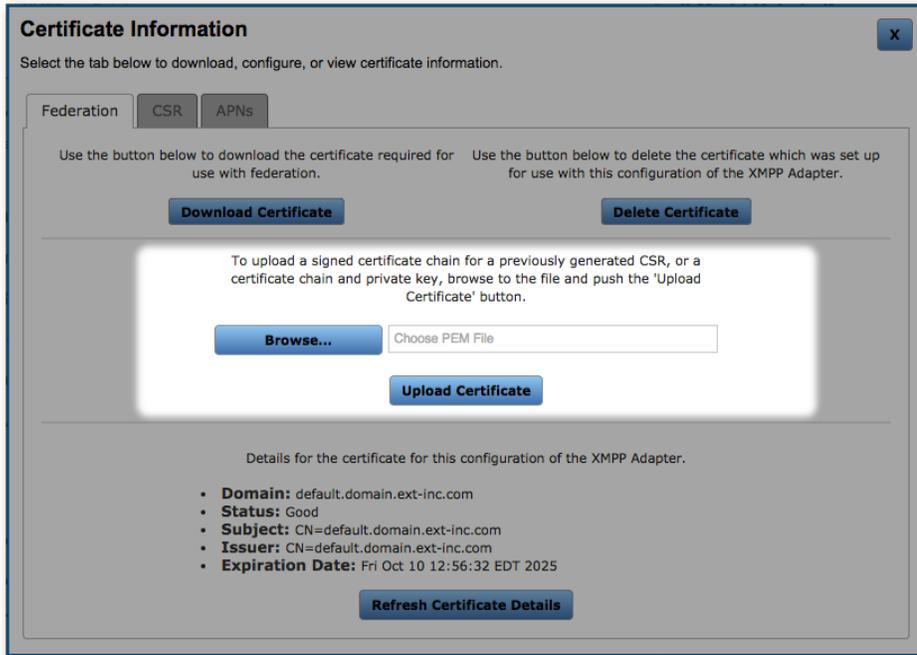
View the Current Certificate Details

Click **Refresh Certificate Details** to display the current configuration certificate details, including the domain of the configuration, the status, subject, issuer of the certificate, and expiration date. The status of the certificate is based upon the expiration date and will use the following statuses:

- Expires Soon - certificate is to expire within a month
- Expired - certificate is past the expired date
- Good - certificate does not expire for a time span greater than a month

When a self-signed certificate expires, a new certificate is generated and replaces the expired certificate. The details of the new certificate will be returned for viewing.
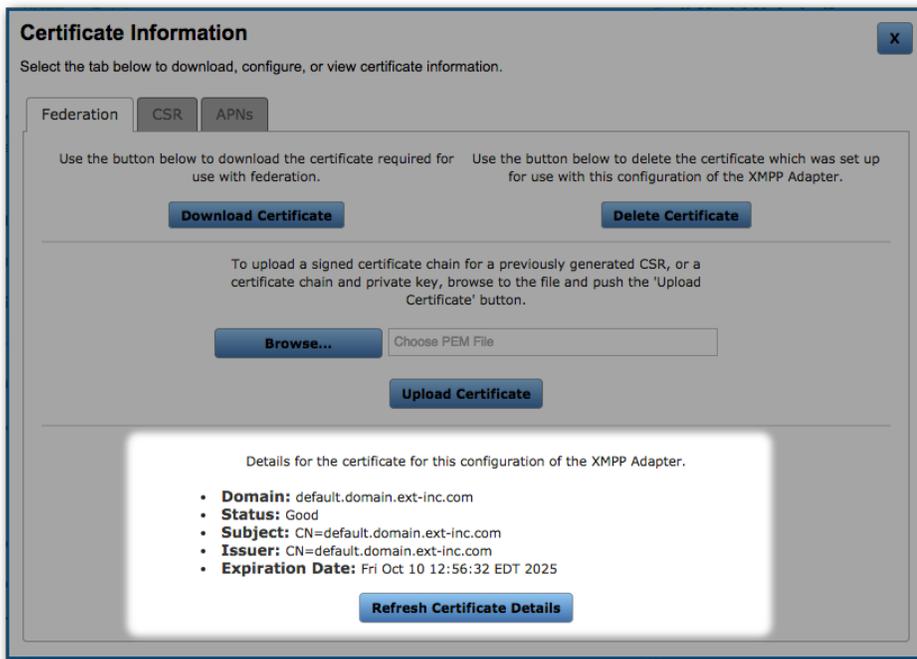
Configuring the CSR

You can configure the Certificate Signing Request in the CSR tab, then download the file and send it to a Certificate Authority (CA) to obtain a signed certificate.

In the Vocera Platform Web Console, navigate to the Vocera XMPP Adapter and view the **Additional Actions** options in the sidebar help section. The following operations can be performed by an administrator from the **XMPP Certificate Manager**.

Complete the fields and click the **Download Certificate Signing Request** link to generate and download a new CSR. All fields must be populated to generate the CSR.

A servlet request is made to create a new CSR, which is returned as a downloadable PEM format file. When the CSR is generated, a self-signed certificate is placed in the "domainName_csr.jks" KeyStore.

The XMPP Certificate Manager displays details about the current CSR in progress, gathered from the self-signed certificate which was stored in the "domainName_csr.jks" KeyStore when a new CSR is generated. These details include: domain name (or common name automatically populated from the domain name), and the country, city, state, organization, and organizational unit configured in the current CSR.

If no current CSR is in progress or downloaded, the details will display as shown below.

Uploading an APNs Certificate

Customers enrolled in the iOS Developer Enterprise Program, who will re-sign and re-distribute the Vocera Vina application, may also want to provide their own APNs (Apple Push Notification service) certificate. To do this, the customer will upload their own push certificate to allow sending APNs messages.

In the Vocera Platform Web Console, navigate to the Vocera XMPP Adapter and view the **Additional Actions** options in the sidebar help section. Click the **XMPP Certificate Manager** link to display this Certificate Information dialog.

Select **Browse** and navigate to the certificate location. The selected filename will populate this field.

Select the **Production Certificate** checkbox if the environment is in production use. This checkbox is to distinguish between the production environment and a testing environment, which does not require as many controls. In the example below, the empty checkbox indicates a non-production environment.

Select the **Next Gen** checkbox when using Next Generation iOS clients. Vocera supports two versions of the APNs clients concurrently, which are authenticated by the respective push certificate. Use this checkbox to authenticate Next Generation iOS clients with a Next Generation certificate. If not checked, the legacy certificate is used for authentication.

Enter a **Password** to verify the certificate.

Select **Upload APNs Certificate**.

Understanding the XMPP Rules

XMPP rules are configured to send conversation, message, and presence information to the Vocera XMPP Adapter when this information is created by an external resource.

See the Vocera Platform Dataset Guide for information about working with rules. See Configuring a Vocera XMPP Adapter on page 52 for information about adapter settings.

The Vocera XMPP Adapter rules can be configured to interact with non-XMPP devices by using virtual sessions to allow them to participate in a conversation.

The XMPP rule configuration options are handled in eight different Rule Action types, each type with its own rule settings. For each of the eight Rule Action types below, a figure displays the Adapter Settings fields and a table provides the details for configuring each field.

In the Adapter Settings, configure the Rule Settings fields to manage message delivery.

Expire Conversation

Select **Expire Conversation** in the Rule Action dropdown menu.

Setting	Description
Conversation	The Jabber ID of the conversation to expire. May contain an attribute expression in the form of #{...}. **This is a required field**.

Leave Conversation

Select **Leave Conversation** in the Rule Action dropdown menu.

Setting	Description
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. It may contain attribute expressions in the form of #{...}. **This is a required field**.
Conversation	The Jabber ID of the conversation. May contain an attribute expression in the form of #{...}. **This is a required field**.

Send Alert

Select **Send Alert** in the Rule Action dropdown menu.

Rule Settings

Rule Action: Send Alert

Recipients:

Re-Alert:

Subject:

Alarm Time:

Message:

Short Message:

Patient MRN:

Event Response Team:

Time-to-Live:

Accept:

Accept Badge Phrases:

Accept and Call:

Callback Number:

Decline:

Decline Badge Phrases:

Store Responding User as:

Additional Content:

Priority Level:

Badge Alert Sound:

Vibrate Enabled:

Audible Alert: ✓

Alert Sound:

Always Play:

Settings	Description
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. If left blank for a Send Alert rule a conference room will be created but no resources will receive a message without an additional Send Invitation rule. It may contain attribute expressions in the form of #{...}. **This is a required field**.
Re-Alert	If checked and a recipient has already received an alert for the same triggering event, the recipient will be notified again based on the priority, audible, and vibration settings in this rule. If not checked and a recipient has already received an alert for the same triggering event, a recipient will not receive a new notification.
Subject	The topic of the conversation room. May contain attribute expression in the form #{...}. Use keywords in this Subject field, as the device display is limited to between 12 and 20 characters. Although this field accepts any entries, the display is truncated depending on the size and number of characters. For example, large size characters such as 'w' take up more space in the Subject display than small size characters such as 'i'. **This is a required field**.
Alarm Time	Use a patient monitor event time in standard solution alarm time; #{alarm_time} or #{alarm_time.as_iso}. An accurate alarm time is critical for aligning the alert with other data, such as waveforms. This field should be left empty if the alert is not for a patient monitor alarm, or if an accurate alarm time is not available.
Message	The message to be shown to recipients. This could be a summary of the information in the workflow page. May contain attribute expressions in the form of #{...}. **This is a required field**.
Short Message	The short message to be played or displayed on a badge. This is an optional text field.
Patient MRN	The MRN of the patient associated with the alert. May contain attribute expressions in the form of #{...}.
Event Response Team	The Jabber IDs of the other resources who are involved in the patient care. May contain attribute expressions in the form of #{...}.
Time-to-Live	The time, in minutes, after which the message is no longer applicable. May be an attribute expression in the form of #{...}, but it must evaluate to an integer. **This is a required field**.
Accept	A list of attribute expression and the values to which to update those attributes when the user clicks on "Accept". Must be in the form of "expression=value", one per line. Expressions are expressed without #{...}. Values may contain other attribute expressions in the form of #{...}.
Accept Badge Phrases	A list of phrases sent to a badge when the user clicks on "Accept". Must be one per line. A total of 5 combined accept and decline phrases can be used.

Settings	Description
Accept and Call	A list of attribute expressions and the values to which to update those attributes when the user clicks on "Accept and Call". Must be in the form "expression=value", one per line. Expressions are expressed without #{...}. Values may contain other attribute expressions in the form of #{...}.
Callback Number	Phone number of the device that will be dialed when the user clicks on 'Accept and Call'.
Decline	A list of attribute expressions and the values to which to update those attributes when the user clicks on 'Decline'. Must be in the form "expression=value', one per line. Expressions are expressed without #{...}. Values may contain other attribute expressions in the form of #{...}.
Decline Badge Phrases	A list of phrases sent to a badge when the user clicks on 'Decline'. Must be one per line. A total of 5 combined accept and decline phrases can be used.
Store Responding User as	The attribute expression describing which dataset to save the responding user name.
Additional Content	Any additional content to be displayed to the user associated with this alert. May contain attributes in the form of #{...}.
Priority Level	The priority of the message.
Badge Alert Sound	The file name of the alert sound to play on a badge.
Vibrate Enabled	Flag to determine if the device should vibrate when a message is sent to the device. Vibrate is not supported on all devices.
Audible Alert	Flag to determine if the device should play an audio alert when a message is sent to the device. Audible alerts ALWAYS play even if the device is not idle.
Alert Sound	The file name of the alert sound to play. This field is only an option if Audible Alert is selected.
Always Play	If checked, the alert sound is played on the device even if the user is marked as Unavailable. This field is only an option if Audible Alert is selected.

Send Alert Custom Parameters

Custom parameters can be used with the XMPP Send Alert Rule. For a full explanation of Custom Parameters, please see the Vocera XMPP Adapter configuration page.

Settings	Descriptions
Parameter	The name of the custom parameter to be added to the alert. Custom parameters allow XMPP alerts to be extended with app specific settings. For example, integration with AirStrip ONE requires the parameters airstripone.bed and airstripone.unit. The value of the custom parameter must be added to the alert if the Parameter is entered. **Custom Parameters are optional, but if a Value is entered, the Parameter is a required field.**
Value	The value to be added to the alert. Custom parameters allow XMPP alerts to be extended with app specific settings. For example, integration with AirStrip ONE requires values of Bed and Unit, (bed1 and ICU for example). The parameter of the customer parameter must be added to the alert if the Value is entered. **Custom Parameters are optional, but if a Parameter is entered, the Value is a required field.**

Send Mass Alert

Select **Send Mass Alert** in the Rule Action dropdown menu.

Settings	Description
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. It may contain attribute expressions in the form of #{...}. **This is a required field.**.
Subject	The topic of the conversation room for the mass alert (e.g. Tornado Warning). May contain attribute expression in the form #{...}. **This is a required field.**
Message	The message to be shown to recipients (e.g., Tornado Warning details: counties affected, duration, etc.). May contain attribute expressions in the form of #{...}. **This is a required field.**
Short Message	The short message to be shown or played on a badge.
Time-to-live	The time in minutes after which the message is no longer applicable. Values must be between 1 and 64800 inclusive (45 days). **This is a required field.**
Additional Content	Any additional content to be displayed to the user associated with this alert.
Priority Level	The priority of the message.
Badge Alert Sound	The file name of the alert sound to play on a badge.
Vibrate Enabled	Flag to determine if the device should vibrate when a message is sent to the device.
Audible Alert	Flag to determine if the device should play an audible alert when a message is sent to the device.
Alert Sound	The file name of the alert sound to play. This field is only an option if Audible Alert is selected.
Always Play	Flag to determine if the device should always play an audible alert when a message is sent to the device, even if the user is in dnd/unavailable mode. This field is only an option if Audible Alert is selected.

Send Mass Alert Custom Parameters

Custom parameters can be used with the XMPP Send Mass Alert Rule. For a full explanation of Custom Parameters, please see the Vocera XMPP Adapter configuration page.

Settings	Descriptions
Parameter	The name of the custom parameter to be added to the alert. Custom parameters allow XMPP alerts to be extended with app specific settings. For example, integration with AirStrip ONE requires the parameters airstripone.bed and airstripone.unit. The value of the custom parameter must be added to the alert if the Parameter is entered. **Custom Parameters are optional, but if a Value is entered, the Parameter is a required field.**
Value	The value to be added to the alert. Custom parameters allow XMPP alerts to be extended with app specific settings. For example, integration with AirStrip ONE requires values of Bed and Unit, (bed1 and ICU for example). The parameter of the customer parameter must be added to the alert if the Value is entered. **Custom Parameters are optional, but if a Parameter is entered, the Value is a required field.**

Send Invitation

Select **Send Invitation** in the Rule Action dropdown menu.

Settings	Descriptions
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. It may contain attribute expressions in the form of #{...}. **This is a required field**.
Re-Alert	If checked and a recipient has already received an alert for the same triggering event, the recipient will be notified again based on the priority, audible, and vibration settings in this rule. If not checked and a recipient has already received an alert for the same triggering event, a recipient will not receive a new notification.
Conversation	The Jabber ID of the conversation. May contain an attribute expression in the form of #{...}. **This is a required field**.
Reason	The reason for the conversation room invitation. May contain an attribute expression the form of #{...}.

Send New/Accept Decline System Message

Select **Send New Accept/Decline System Message** in the Rule Action dropdown menu.

Settings	Descriptions
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. It may contain attribute expressions in the form of #{...}. **This is a required field**.
From	The single Jabber ID of the resource who sent the message. Ignored if marked as a system message. May contain attribute expressions in the form of #{...}. **This is a required field**.
Accept Message	If checked, the message is accepted; if not, the message is declined.

Send New Message

Select **Send New Message** in the Rule Action dropdown menu.

Settings	Descriptions
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. It may contain attribute expressions in the form of #{...}. **This is a required field**.

Settings	Descriptions
From	The single Jabber ID of the resource who sent the message. Ignored if marked as a system message. May contain attribute expressions in the form of #{...}. **This is a required field**
Message	The message to be shown to the recipients. This could be a summary of the information in the workflow page. May contain attribute expressions in the form of #{...}. **This is a required field**.
Short Message	The short message to be played or displayed on a badge.

Send New System Message

Select **Send New System Message** in the Rule Action dropdown menu.

Settings	Descriptions
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. It may contain attribute expressions in the form of #{...}. **This is a required field**.
Message	The message to be shown to the recipients. This could be a summary of the information in the workflow page. May contain attribute expressions in the form of #{...}. **This is a required field**.
Short Message	The short message to be played or displayed on a badge.

Start Conversation

Select **Start Conversation** in the Rule Action dropdown menu.

Settings	Descriptions
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. If left blank for a Send Alert rule a conference room will be created but no resources will receive a message without an additional Send Invitation rule. It may contain attribute expressions in the form of #{...}. **This is a required field**.
Subject	The topic of the conversation room. May contain attribute expression in the form #{...}. Use keywords in this Subject field, as the device display is limited to between 12 and 20 characters. Although this field accepts any entries, the display is truncated depending on the size and number of characters. For example, large size characters such as 'w' take up more space in the Subject display than small size characters such as 'i'. **This is a required field**.

Update Presence

Select **Update Presence** in the Rule Action dropdown menu.

| Settings	Descriptions
Recipients	A list of Jabber IDs or logins of the resources who will receive the message. For sending a new message to an existing conference room, use the Jabber ID of the room. It may contain attribute expressions in the form of #{...}. **This is a required field**.
Presence Type	The Presence Type to be set. The options are Available, Unavailable, or Offline. **This is a required field**.

Integrating an AirStrip One Application

Vocera Vina is capable of integration with the AirStrip One application if the facility uses it to view patient data.

If the AirStrip One application is used in a facility, specific configurations are required in order for Vocera Platform to properly transfer patient data into the application.

AirStrip One integration is not a part of the standard Vocera Platform EMDAN solution. Custom parameters must be added to the Vocera XMPP Adapter for AirStrip One integration to function with Vocera Vina alerts. The endpoint devices must also be registered with AirStrip One for integration with Vocera Platform.

On the adapter level, a shared key parameter needs to be created to establish an external connection. More parameters are created to share alert level data across applications. See Configuring a Vocera XMPP Adapter on page 52 to access configuration information for **Custom Parameters**.

In this example, a shared parameter is established with AirStrip One, and also sending across facility, unit, and bed information. Different parameters may be required upon installation.
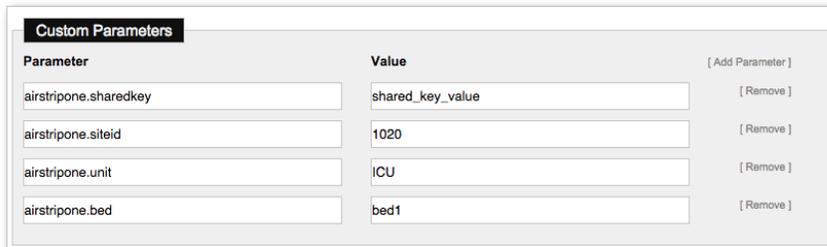
Custom Parameters		
Parameter	**Value**	[Add Parameter]
airstripone.sharedkey	shared_key_value	[Remove]
airstripone.siteid	1020	[Remove]
airstripone.unit	ICU	[Remove]
airstripone.bed	bed1	[Remove]

Implementing an XMPP Environment

Implementation tips are provided here for creating the proper environment to support XMPP devices.

Vocera XMPP Adapter Configuration

Multiple instances of the Vocera XMPP Adapter can be created, however, only one instance can be active at a time.

XMPP traffic on the Internet and hospital networks between our appliance and devices over port 5222 is secured by SSL. Vocera Platform supports the capability of multiple proxy servers, with one proxy server per data center in a facility.

The Vocera XMPP Adapter enables XMPP communication between Vocera users using XMPP clients by acting as the XMPP server for its configured domain. The Vocera XMPP Adapter supports communication with federated users on other XMPP domains. A self-signed security certificate generated by the Vocera XMPP Adapter must be uploaded to the federated server for federation services to function.

Chat Domain Hostnames

The Vocera XMPP Adapter connects to the server from the Vocera Platform client using a domain such as `user@mydomain.com`, where mydomain.com is the server hostname. You must have a static IP address with an entry in DNS for mydomain.com.

Register the following A records in DNS:

- mydomain.com
- chat.mydomain.com (only required if implementing federation)
- extension.mydomain.com (only required if implementing federation)
- patients.mydomain.com (only required if implementing federation)

Register the following SRV records in DNS. These SRV records are not required, but they are recommended for XMPP installations. They allow the server host name to be different than the XMPP domain.

_xmpp-server._tcp.mydomain.com 0 0 5269 mydomain.com.

_xmpp-server._tcp.chat.mydomain.com 0 0 5269 mydomain.com.

_xmpp-server._tcp.extension.mydomain.com 0 0 5269 mydomain.com.

_xmpp-client._tcp.mydomain.com 0 0 5222 mydomain.com.

_xmpp-client._tcp.chat.mydomain.com 0 0 5222 mydomain.com.

_xmpp-client._tcp.extension.mydomain.com 0 0 5222 mydomain.com.

_xmpp-server._tcp.patients.mydomain.com 0 0 5269 mydomain.com.

_xmpp-client._tcp.patients.mydomain.com 0 0 5222 mydomain.com.

XMPP User Presence

Each facility must determine the presence states required for their Vocera Platform implementation, such as Available and Unavailable; see **Manage Presence States** to create the required presence states.

The presence of an individual XMPP user will be set automatically when a user logs in or logs out of the application. Within the Vocera Vina application, a user may set their own status by choosing from among the list of defined presence states for the facility. Additionally, an administrator may set the presence state of an individual user; see **Manage User Presence** in the Vocera Platform Workflow Guide.

The Vocera XMPP Adapter calculates a user's overall presence by using the current highest priority device presence (Available > Unavailable > Offline).

When Vocera users are logged into multiple devices, the Vocera XMPP Adapter stores the statuses for the user's devices. The user's presence status is aggregated from the combined devices and the highest priority status is used for presence updates. For example, an 'Available' presence status is prioritized over an 'Unavailable' status on another device; the user's presence is unavailable when all devices the user is logged into are marked as Unavailable, or when logged into only the Desktop.

User Presence Rule Configuration

Users with devices that are not XMPP-enabled, such as Cisco or Vocera, have a presence of Offline because these users do not have an active session. The presence rule provides the ability to set a user online via a virtual session.

In a Vocera Platform dataset, create a rule or select a rule to edit, and then select **XMPP** in the adapter field. The Adapter Settings will automatically display the **Rule Settings** section shown below.

Select the **Update Presence** option in the Rule Action drop down menu to display the following configuration fields. Setting the presence type to "Available" and triggering the rule for updating the user's presence will create a virtual user session if there are no resources for the sender. When the presence type is set to "Offline", the unavailable presence will send the user (regardless of session type) offline by destroying the session.

- **Rule Action**: Select the Update Presence option to support updating a user's presence.
- **Recipients**: Enter the Jabber ID of a user or an existing conference room to receive a message. May contain attribute expressions of the form #{...}.
- **Presence Type**: Select the presence type; Available, Unavailable, Offline. When Available or Unavailable are selected, the Status field displays.

- **Status**: Enter the value of the status to set.

XMPP Workflow Integration

Vocera allows users to send and receive messages and to manage their alerts using workflow phones, such as Cisco and SpectraLinkXML devices, via configuration of the Vocera Platform datasets, rules, and views. Vocera Vina applications provide an enhanced user experience via XMPP for holding conversations between smartphone device users. When a deployment integrates a combination of workflow phones and smartphones using XMPP in the facility, the Vocera configuration requires seamless communication between the different device types. Users should not be aware that they are communicating with someone who is using a different type of device.

Component States for the Messaging Environment

The solution configuration for messaging will differ significantly when:

- the installation includes only workflow phones
- the installation includes only XMPP devices
- the installation is intended to integrate both workflow phones and XMPP devices

The table below indicates the required state of several components based on the desired functionality:

Component / Messaging	Workflow Only	Integrated	XMPP Only
Workflow device adapter (CUCM, SpectraLinkXML, Smartphone)	enabled	enabled	**disabled**
XMPP adapter	**disabled**	enabled	enabled
Data Update for XMPP	**disabled**	enabled	**disabled**
DM/<Vendor>Group rules	enabled	**disabled**	**disabled**

In an integrated environment, where both workflow and XMPP devices are used, all group messages will pass through an XMPP chat room regardless of the device type each member of the group is assigned. Device Messaging/Vendor-specific Group rules must be disabled in an integrated environment. If the DM/<Vendor>Group rules are enabled in an integrated environment, the users on workflow phones will receive some duplicate messages. Workflow phone users will get each message sent to the group twice; once directly, and once filtered through the XMPP conversation.

DataUpdate for XMPP Adapter

Implement the **DataUpdate for XMPP adapter** when the facility will be using a combination of workflow devices (such as Cisco, SpectraLinkXML, and smartphone) and XMPP devices for messaging in the production environment. This adapter should not be enabled for installations that do not use both XMPP and workflow devices; when an adapter is not active, its associated rules will not be triggered.

The DataUpdate for XMPP adapter encapsulates all DataUpdate rules needed for XMPP integration. These DataUpdate rules assist in managing the presence states of users with workflow devices, such as Cisco, SpectraLinkXML and smartphone, and in creating device messages for XMPP-to-workflow phone communication. The Vocera XMPP Adapter cannot write records to the Messages dataset unless the presence of the user is available, therefore, install the DataUpdate for XMPP adapter to allow workflow devices and XMPP devices to communicate.

Note: If Rules are configured in a way that multiple rules fire for the same alert at the same time, some messages may not be delivered.

Workflow User Presence

Users with workflow phones will go online when they log into a device, and offline when they log out of a device.

If a user logs into a workflow device that currently has a user associated, the previous user may not go offline. In this case, an administrator should assign the correct presence (offline) for the previous user; see **Manage User Presence** in the Vocera Platform Workflow Guide.

An administrator may also set a user online or offline by changing the association of a user to a device; see **Manage Phones** in the Vocera Platform Workflow Guide.

Configuring the Edge Proxy Server

Vocera's Edge proxy server is the intermediate point between a user's Internet connected mobile device and the Vocera Platform server.

A proxy server is a dedicated machine that behaves as a secure intermediary between an endpoint and another server from which a user is requesting service. Edge facilitates secure messaging used in the Vocera Platform appliance by intercepting XMPP requests and then verifying their fulfillment. Edge communicates with a network switch to pass on XMPP requests to the Vocera Platform server.

Shown below is a diagram of how the Edge proxy server fits into a typical networking infrastructure model. The Edge server positions itself between networks in the demilitarized zone and securely facilitates external facing services of the Vocera Platform, such as XMPP requesting, to the Internet. The following explains how to access the Edge server configuration menu and how Edge should be configured into the Vocera Platform appliance.
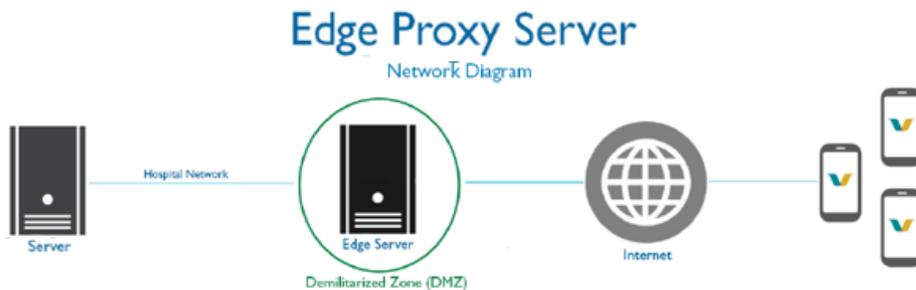
Minimum Requirements

The Vocera Edge server requires the following components at the minimum in order to properly function inside the facility:

- 2048 MB memory
- 1 16 GB HDD
- 1 Central Processing Unit (CPU) core
- 1 video card
- 1 Virtual Machine Communication Interface (VMCI)
- 1 CD/DVD drive
- 1 network adapter

Multiple Edge proxy servers may be configured for a single facility. A multiple proxy environment enables a high level of availability for users accessing Vocera Vina from outside of the hospital network. Should a Vocera Vina XMPP client fail to connect to an Edge server while in a multiple proxy environment, another connection attempt will automatically be made to a different Edge server in the network until a successful connection is established. The facility's IT support must configure their own DNS entries for all Edge servers in deployment.

Vocera provides an 'administrator' account that is shared with the facility to allow access to the Edge appliance for future configuration updates since remote access is not available. After the initial 'administrator' log in, the default password (given by Vocera) must be changed and securely stored for future use, either by the facility's IT personnel in a safe location or by Vocera via Salesforce. The login using 'administrator' will directly launch the configuration menu; command line access will not be accessible from this account. The new Edge appliance password storage location is at the discretion of the Implementation Specialist. It is imperative that the default password is changed so that the network security Edge provides is not compromised. An internal administrative account is available for initial configuration and is never shared with the facility. This administrative account supersedes the facility-level 'administrator' account with unique privileges, including command line access.

To open the configuration menu, navigate to the Edge appliance within a VMware client or be physically present at the machine and log into the 'administrator' account. If the Vocera administrative account is being used, run 'sudo xmpp-proxy-setup' at the command line interface.

The configuration menu has five options that must be configured to work with the appliance: **Network**, **XMPP**, **Route**, **NTP**, and **Timezone**. On the keyboard, use the up/down arrow keys to navigate around the options and the left/right arrow keys to choose between Select and Exit, and the Enter key to select an available option.

> ⚠️ **Warning:** The Edge appliance may not, under any circumstances, be accessed across the network for the purpose of maintenance. For security reasons, Edge may only be accessed directly via the console. The 'administrator' account must be used by the facility's IT personnel for configuration updates after the initial setup is completed.
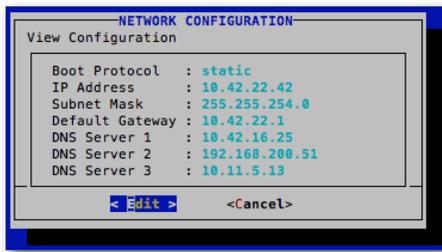
Network

Select **Network** to edit Edge's network configuration. This information establishes the identity of the Edge server within the network.
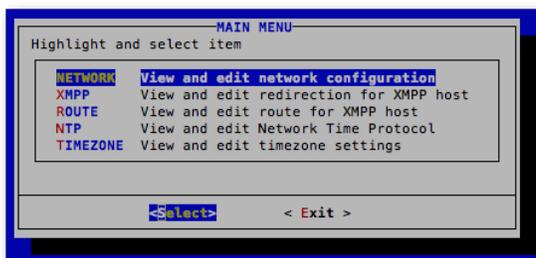
Enter the network information for the Edge server into the appropriate fields and select **Submit** when done.
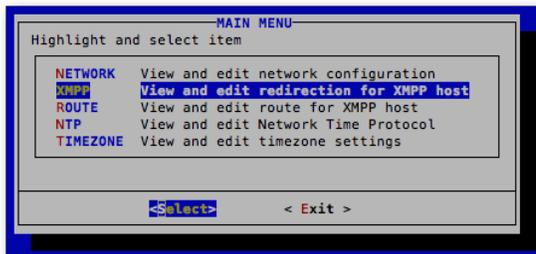
> 📝 **Note:** The Edge server uses Network Protocol Time which involves referencing a host name. A DNS server must be configured in order to properly resolve host names.
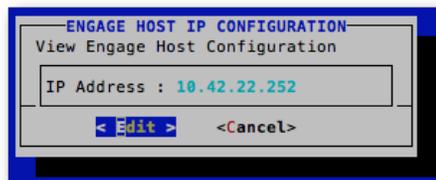
```
┌───────NETWORK CONFIGURATION───────┐
│ View Configuration                │
│                                   │
│    Boot Protocol   : static       │
│    IP Address      : 10.42.22.42  │
│    Subnet Mask     : 255.255.254.0│
│    Default Gateway : 10.42.22.1   │
│    DNS Server 1    : 10.42.16.25  │
│    DNS Server 2    : 192.168.200.51│
│    DNS Server 3    : 10.11.5.13   │
│                                   │
│        < Edit >       <Cancel>    │
│                                   │
└───────────────────────────────────┘
```

XMPP

Select **XMPP** to edit the IP address of the client server. This address allows the Edge server to communicate with the client network.
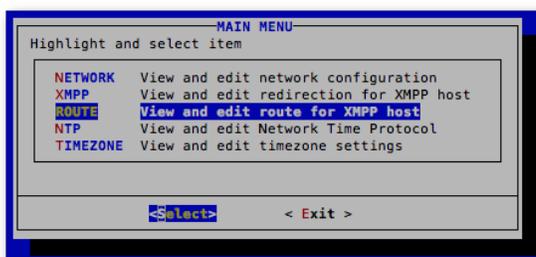
```
┌────────────MAIN MENU────────────┐
│ Highlight and select item       │
│                                  │
│    NETWORK    View and edit network configuration    │
│    XMPP       View and edit redirection for XMPP host│
│    ROUTE      View and edit route for XMPP host      │
│    NTP        View and edit Network Time Protocol    │
│    TIMEZONE   View and edit timezone settings        │
│                                  │
│          <Select>       < Exit > │
│                                  │
└──────────────────────────────────┘
```

Enter the desired IP address in the available field. Select **Submit** when done.

```
┌──────ENGAGE HOST IP CONFIGURATION──────┐
│ View Engage Host Configuration         │
│                                        │
│  IP Address : 10.42.22.252             │
│                                        │
│        < Edit >       <Cancel>         │
│                                        │
└────────────────────────────────────────┘
```
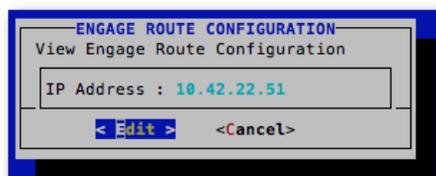
Route

Select **Route** to configure the IP address if the facility uses a dual firewall connection. This enables communication with a network switch if one is in use.
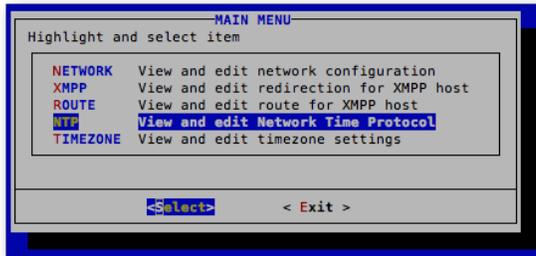
```
┌────────────MAIN MENU────────────┐
│ Highlight and select item       │
│                                  │
│    NETWORK    View and edit network configuration    │
│    XMPP       View and edit redirection for XMPP host│
│    ROUTE      View and edit route for XMPP host      │
│    NTP        View and edit Network Time Protocol    │
│    TIMEZONE   View and edit timezone settings        │
│                                  │
│          <Select>       < Exit > │
│                                  │
└──────────────────────────────────┘
```

Enter the desired IP address in the available field. Select **Submit** when done.

```
┌──────ENGAGE ROUTE CONFIGURATION──────┐
│ View Engage Route Configuration      │
│                                      │
│  IP Address : 10.42.22.51            │
│                                      │
│        < Edit >       <Cancel>       │
│                                      │
└──────────────────────────────────────┘
```
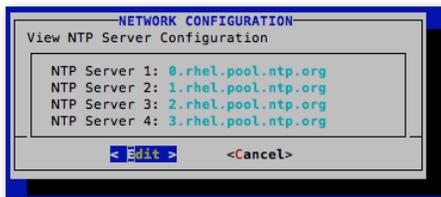
NTP

Select **NTP** to edit the Network Time Protocol (NTP) server addresses. The NTP ensures the server's timestamp remains calibrated within milliseconds within the Coordinated Universal Time (UTC).
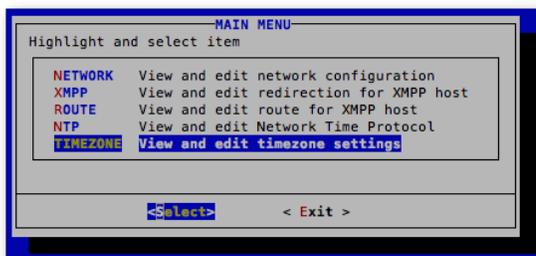
```
┌──────────MAIN MENU──────────┐
│Highlight and select item                       │
│                                                 │
│   NETWORK   View and edit network configuration │
│   XMPP      View and edit redirection for XMPP host │
│   ROUTE     View and edit route for XMPP host   │
│   NTP       View and edit Network Time Protocol │
│   TIMEZONE  View and edit timezone settings     │
│                                                 │
│                                                 │
│          <Select>        < Exit >               │
│                                                 │
└─────────────────────────────────────────────────┘
```

Enter the desired NTP server(s) in the available fields. Select **Submit** when done.

```
┌──────NETWORK CONFIGURATION──────┐
│View NTP Server Configuration                │
│                                             │
│   NTP Server 1: 0.rhel.pool.ntp.org         │
│   NTP Server 2: 1.rhel.pool.ntp.org         │
│   NTP Server 3: 2.rhel.pool.ntp.org         │
│   NTP Server 4: 3.rhel.pool.ntp.org         │
│                                             │
│        < Edit >        <Cancel>             │
│                                             │
└─────────────────────────────────────────────┘
```

Timezone

Select **Timezone** to edit the Edge time zone configuration.

```
┌──────────MAIN MENU──────────┐
│Highlight and select item                       │
│                                                 │
│   NETWORK   View and edit network configuration │
│   XMPP      View and edit redirection for XMPP host │
│   ROUTE     View and edit route for XMPP host   │
│   NTP       View and edit Network Time Protocol │
│   TIMEZONE  View and edit timezone settings     │
│                                                 │
│                                                 │
│          <Select>        < Exit >               │
│                                                 │
└─────────────────────────────────────────────────┘
```

Select the time zone region where your facility resides. If your specific city is not in the available list, please select the nearest present city. Select **Submit** when done.

```
┌──────────TIMEZONE──────────┐
│Press spacebar to select new time zone:      │
│                                             │
│        ( ) America/Adak                     │
│        ( ) America/Anchorage                │
│        ( ) America/Chicago                  │
│        ( ) America/Denver                   │
│        ( ) America/Los_Angeles              │
│        (*) America/New_York                 │
│        ( ) America/Phoenix                  │
│        ( ) America/Puerto_Rico              │
│        ( ) Pacific/Guam                     │
│        ( ) Pacific/Honolulu                 │
│        ↓(+)                      90%         │
│                                             │
│          <Submit>        <Cancel>           │
│                                             │
└─────────────────────────────────────────────┘
```
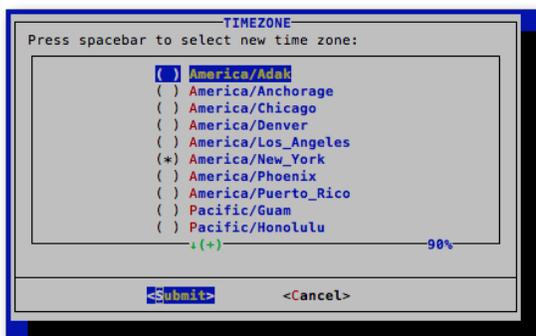
Configuring the Federated Server to Work with Vocera Platform

The basic requirements to federate are met by setting up hostnames in DNS and adding the Vocera XMPP Adapter certificate to the Cisco Unified Communications Manager IM and Presence server.

The Cisco Unified Communications Manager IM and Presence platform facilitates the secure exchange of presence and instant messaging (IM) information between Cisco Unified Communications Manager and the Vocera XMPP Adapter.

> **Note:** Vocera XMPP Adapter integration with CUCM 9.0 is optional and is not required for the Vocera XMPP Adapter to function.

Register Hostnames in DNS

The domains listed on this page use mydomain.com to represent the XMPP server domain.

The following domains must be registered in DNS for federation between servers.

A record for:

- mydomain.com
- chat.mydomain.com
- extension.mydomain.com

The following hostnames should be registered in DNS.

SRV records for:

_xmpp-server._tcp.mydomain.com 0 0 5269 mydomain.com.

_xmpp-server._tcp.chat.mydomain.com 0 0 5269 mydomain.com.

_xmpp-server._tcp.extension.mydomain.com 0 0 5269 mydomain.com.

_xmpp-client._tcp.mydomain.com 0 0 5222 mydomain.com.

_xmpp-client._tcp.chat.mydomain.com 0 0 5222 mydomain.com.

_xmpp-client._tcp.extension.mydomain.com 0 0 5222 mydomain.com.

Upload the XMPP Certificate to the Cisco Unified Communications Manager IM and Presence Server

The Vocera XMPP Adapter generates a self-signed security certificate required to communicate with it, which specifies the XMPP server domain. The certificate must then be uploaded to the Cisco Unified Communications Manager IM and Presence for the server to trust the Vocera XMPP Adapter and allow federation.

Once the certificate is generated and downloaded as described in Federating the Servers on page 59, then the certificate must be uploaded to Certificate Management in the Presence OS Administration on the Cisco Unified Communications Manager IM and Presence server. If a certificate later has to be re-generated, replace the XMPP certificate on the Cisco Unified Communications Manager IM and Presence server and restart the Cisco Unified Communications Manager IM and Presence service and the Federation services.

Set Security in Cisco Unified CM IM and Presence Administration

Navigate to **Unified CM IM and Presence Administration** and log in with credentials provided by a System Administrator.

Navigate the following path, as shown below: **Presence > Inter-Domain Federation > XMPP Federation > Settings**. Ensure the following are enabled in **Security Settings**:

- Security Mode: TLS Required
- Require client-side security certificates
- Enable SASL EXTERNAL on all incoming connections
- Enable SASL EXTERNAL on all outgoing connections
- Dialback Secrets are needed when there is a certificate issue. Vocera Platform and Cisco Unified Communications Manager IM and Presence will prefer SASL security. See Upload Certificate in Cisco Unified Communications Manager IM and Presence Operating System Administration below.
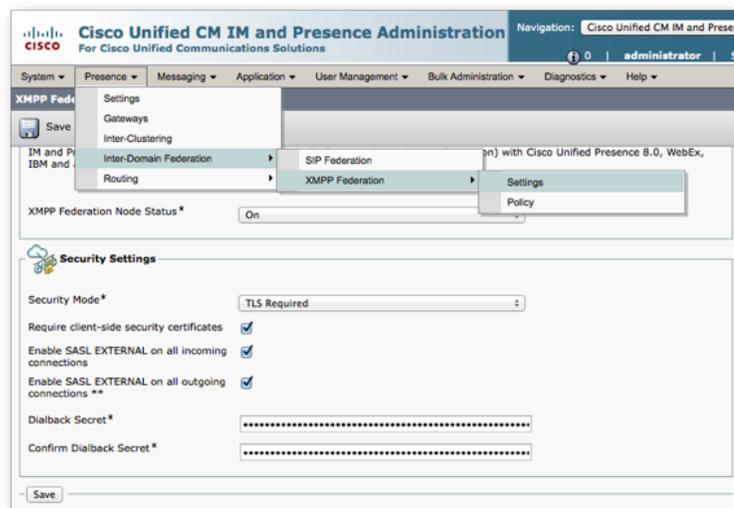
Navigate the following path, as shown below: **Presence > Inter-Domain Federation > XMPP Federation > Policy**. Ensure the XMPP Federation Default Policy is set to **Allow**. If the XMPP Federation Policy is set to **Deny**, then ensure the Vocera Platform hostname is listed in the **XMPP Federation Policy Exception** field.
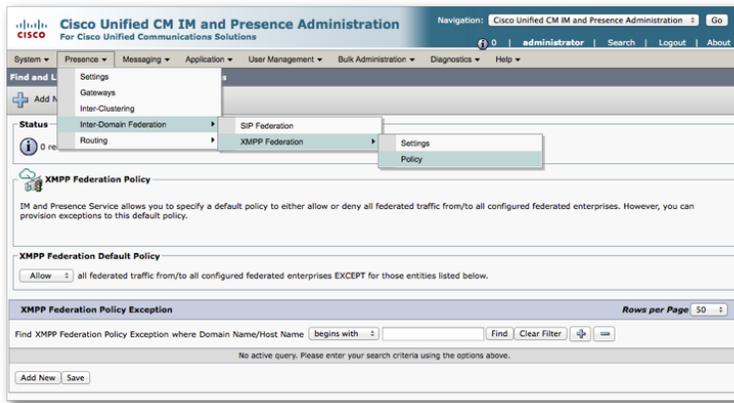
Upload Certificate in Cisco Unified IM and Presence Operating System Administration

Navigate to **Cisco Unified IM and Presence Operating System Administration** on the Cisco Unified Communications Manager IM and Presence server and log in with the credentials provided by a System Administrator.
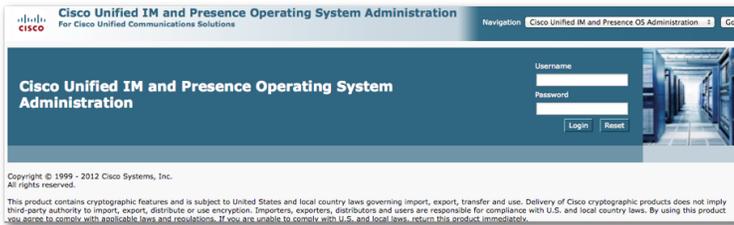
Select **Security > Certificate Management** in the menu bar, as shown below. Use Find to view existing certificates. Select **Upload Certificate/Certificate Chain** and upload the XMPP self-signed certificate. If a certificate already exists for the host, you must remove it. See Replace an Existing XMPP Certificate on the Cisco Unified Communications Manager IM and Presence Server below.
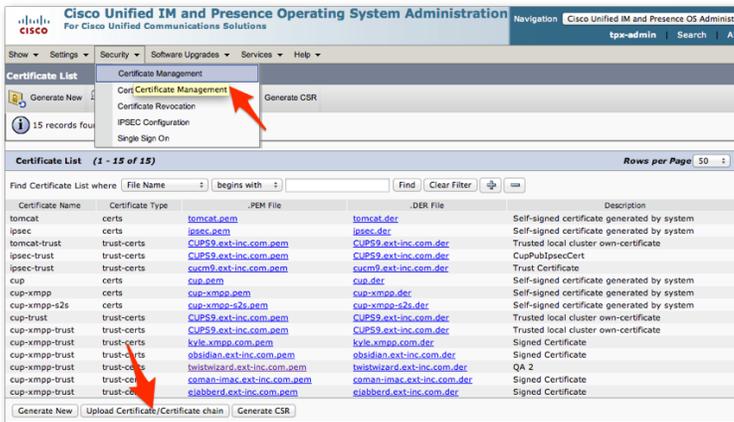
Select **cup-xmpp-trust** in the Certificate Name drop-down list and enter a meaningful identification statement in the Description field. Select **Choose File** and navigate to the .pem certificate file downloaded from the Vocera XMPP Adapter. Click **Upload File** to load the XMPP certificate to the Cisco Unified Communications Manager IM and Presence server.

Replace an Existing XMPP Certificate on the Cisco Unified Communications Manager IM and Presence Server

Under some circumstances the Vocera XMPP Adapter will generate a new certificate, and the old certificate will no longer work. This may happen if the domain name changes, for example.

Select the old certificate and delete it, then generate and upload a new certificate using the steps above.

Warning: If the Vocera XMPP Adapter log contains the following error, upload a new XMPP security certificate:

```
2013-10-09 10:47:29,473 [pool-40-thread-2] INFO : error caught on transportation layer
javax.net.ssl.SSLHandshakeException: SSL handshake failed.
at org.apache.mina.filter.ssl.SslFilter.messageReceived(SslFilter.java:487)
at
 org.apache.mina.core.filterchain.DefaultIoFilterChain.callNextMessageReceived(DefaultIoFilterCh
at org.apache.mina.core.filterchain.DefaultIoFilterChain.access
$1200(DefaultIoFilterChain.java:47)
at org.apache.mina.core.filterchain.DefaultIoFilterChain$EntryImpl
$1.messageReceived(DefaultIoFilterChain.java:765)
at
 org.apache.mina.core.filterchain.IoFilterAdapter.messageReceived(IoFilterAdapter.java:109)
at
 org.apache.mina.core.filterchain.DefaultIoFilterChain.callNextMessageReceived(DefaultIoFilterCh
at
 org.apache.mina.core.filterchain.DefaultIoFilterChain.fireMessageReceived(DefaultIoFilterChain.
at
 org.apache.mina.core.polling.AbstractPollingIoProcessor.read(AbstractPollingIoProcessor.java:7
at
 org.apache.mina.core.polling.AbstractPollingIoProcessor.process(AbstractPollingIoProcessor.java
at
 org.apache.mina.core.polling.AbstractPollingIoProcessor.process(AbstractPollingIoProcessor.java
at org.apache.mina.core.polling.AbstractPollingIoProcessor.access
$600(AbstractPollingIoProcessor.java:67)
at org.apache.mina.core.polling.AbstractPollingIoProcessor
$Processor.run(AbstractPollingIoProcessor.java:1124)
at org.apache.mina.util.NamePreservingRunnable.run(NamePreservingRunnable.java:64)
at java.util.concurrent.ThreadPoolExecutor$Worker.runTask(ThreadPoolExecutor.java:886)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:908)
at java.lang.Thread.run(Thread.java:662)
Caused by: javax.net.ssl.SSLException: Received fatal alert: unknown_ca
at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Alerts.java:190)
```

```
at com.sun.net.ssl.internal.ssl.SSLEngineImpl.fatal(SSLEngineImpl.java:1429)
at com.sun.net.ssl.internal.ssl.SSLEngineImpl.fatal(SSLEngineImpl.java:1397)
at com.sun.net.ssl.internal.ssl.SSLEngineImpl.recvAlert(SSLEngineImpl.java:1563)
at com.sun.net.ssl.internal.ssl.SSLEngineImpl.readRecord(SSLEngineImpl.java:1023)
at com.sun.net.ssl.internal.ssl.SSLEngineImpl.readNetRecord(SSLEngineImpl.java:837)
at com.sun.net.ssl.internal.ssl.SSLEngineImpl.unwrap(SSLEngineImpl.java:713)
at javax.net.ssl.SSLEngine.unwrap(SSLEngine.java:607)
at org.apache.mina.filter.ssl.SslHandler.unwrap(SslHandler.java:728)
at org.apache.mina.filter.ssl.SslHandler.unwrapHandshake(SslHandler.java:666)
at org.apache.mina.filter.ssl.SslHandler.handshake(SslHandler.java:552)
at org.apache.mina.filter.ssl.SslHandler.messageReceived(SslHandler.java:351)
at org.apache.mina.filter.ssl.SslFilter.messageReceived(SslFilter.java:468)
```

Restart the Presence Services

Restart the presence services when a new certificate has been uploaded, but the domain name does not change.

Log into **Cisco Unified IM and Presence Serviceability** on the Cisco Unified Communications Manager IM and Presence server, as shown below. Select **Tools > Control Center - Feature Services** in the menu bar. Then, restart the **Cisco Presence Engine** and the **Cisco XCP XMPP Federation Connection Manager** services.

Understanding Adapter Installation

Adapters are installed on the Vocera Platform in a solution package, or individually as needed by the customer.

The Vocera Platform uses adapters to integrate with external systems and devices. Each adapter is configured by the user to include information that will allow the Vocera Platform to communicate and interact with a specific type of resource and, depending on the adapter, devices that resource may control. Adapters can allow the Vocera Platform to monitor and collect data, as well as send data out, when triggered manually or automatically.

When implementing Vocera Platform at a customer site, use this document to install an adapter that is not supplied in the Gold Image. Otherwise, you will install a needed adapter when instructed in the solution package installation process described in the Vocera Platform Installation Guide.

Recreating a Repository

In the event that the repository reference file has been compromised, you can re-create the platform repository.

This information should be specified on the related adapter's Release Information page in the wiki. See **Releases** and navigate to the needed adapter.

1. Verify that the adapter resides in a repository which is in '**/etc/yum.repos.d/**'.
2. If the **repolist** or **yum** commands fail, verify that the file exists and try again. For example, use the following code to verify the repository exists on the Vocera Platform appliance:

   ```
   [tpx-admin@engage log]$ cat /etc/yum.repos.d/vocera.repo
   ```
3. Verify the output appears as shown.

   ```
   #-------------------------------------------------------------------------------
   # NOTICE: Only use the General Availability (platform-6.X-ga) repository for customer
    deployments.
   # Use of Controlled Release (platform-6.X-cr) or Software Quality Assurance
    (platform-6.X-sqa) in
   # accordance to process QOP-75-01 Production Work Order and History Record, contact
    your
   # manager for questions.
   #-------------------------------------------------------------------------------
   [Platform-6.0]
   name=Platform-6.0
   baseurl=https://box.voceracommunications.com/Platform-6.0-GA
   enabled=1
   gpgcheck=0
   ```

Installing an Adapter

Install or uninstall a Vocera Platform adapter at a customer site on a Vocera system for a customer.

Execute the following steps using the system's command prompt.

1. Verify that the adapter resides in a repository which is in '**/etc/yum.repos.d/**'.
2. Run the following commands:

```
sudo yum clean all
sudo yum check-updates
```

3. Verify that the rpm package to be installed is available using the following command:

```
sudo yum list available | grep extension
```

4. Install the adapter by specifying its rpm package name in place of <package-name> in the code below. (This information should be specified on the related Release Information page in the wiki; see **Release Notes**.)

```
sudo yum install <package-name>
```

5. Uninstall an adapter by specifying its rpm package name in place of <package-name> in the code below. (This information should be specified on the related Release Notes page; see **Release Notes**.)

```
sudo yum remove <package name>
```

Practicing an Adapter Installation

Replicate these steps using the needed adapter package, in order to install adapters other than the example given here.

1. Verify the repo file contains the repos up to and including the release of interest.

```
[tpx-admin@engage log]$ cat /etc/yum.repos.d/vocera.repo
#---------------------------------------------------------------------------
# NOTICE: Only use the General Availability (platform-6.X-ga) repository for customer
 deployments.
# Use of Controlled Release (platform-6.X-cr) or Software Quality Assurance
 (platform-6.X-sqa) in
# accordance to process QOP-75-01 Production Work Order and History Record, contact
 your
# manager for questions.
#---------------------------------------------------------------------------
[Platform-6.0]
name=Platform-6.0
baseurl=https://box.voceracommunications.com/Platform-6.0-GA
enabled=1
gpgcheck=0
```

2. Execute the following commands:

```
[tpx-admin@engage log] $ sudo yum check-updates
Loaded plugins: langpacks, product-id, subscription-manager
This system is not registered to Red Hat Subscription Management. You can use
 subscription-manager to register.
Quartz
                                                | 3.6 kB  00:00:00
(1/2): Quartz/group_gz
                                                |  483 B  00:00:00
(2/2): Quartz/primary_db
                                                |  29 kB  00:00:00
```

3. Verify the package is available, using the following command:

```
[tpx-admin@engage log] $ sudo yum list available | grep extension
   extension-navicare-interface.x86_64                    1.3.6-0              Platform 5.0
```

4. Install the needed adapter; in this example, install the Navicare adapter:

```
[tpx-admin@engage log] $ sudo yum install extension-navicare-interface
Loaded plugins: langpacks, product-id, subscription-manager
This system is not registered to Red Hat Subscription Management. You can use
 subscription-manager to register.
Resolving Dependencies
--> Running transaction check
---> Package extension-navicare-interface.x86_64 0:1.3.6-0 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                               Arch
 Version                    Repository                        Size
================================================================================
Installing:
 extension-navicare-interface                     x86_64
 1.3.3-0                    Quartz                            59 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 59 k
Installed size: 62 k
Is this ok [y/d/N]: y
Downloading packages:
extension-navicare-interface-1.3.6-0.x86_64.rpm
                                          |  59 kB   00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : extension-navicare-interface-1.3.6-0.x86_64
                                                            1/1
  Verifying  : extension-navicare-interface-1.3.6-0.x86_64
                                                            1/1


Installed:
  extension-navicare-interface.x86_64 0:1.3.6-0


  Complete!
```

5. This completes the steps to install an adapter.

Navigating the Vocera Platform Adapters

Access the Adapters tab and use the filter or search tools to display a specific adapter.

This page is used by all the adapter guides, and therefore, the adapter used as an example here may not be the adapter that you are working with currently.

1. Access the Vocera Platform Web Console and sign in with your system credentials.
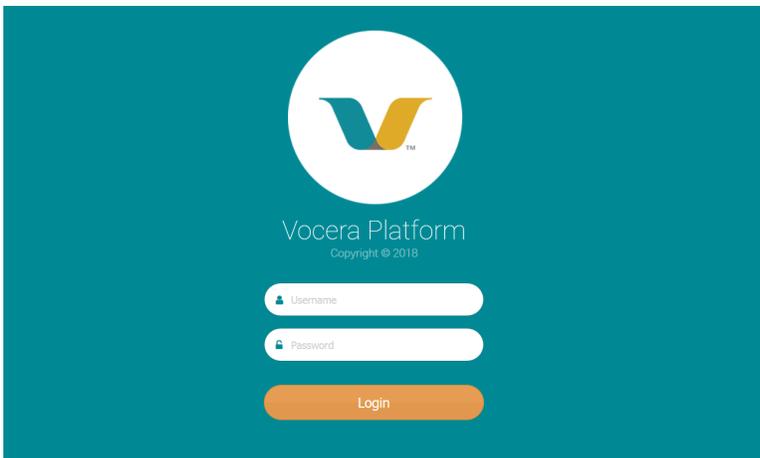
2. Select **Settings > Adapters** in the navigation menu.
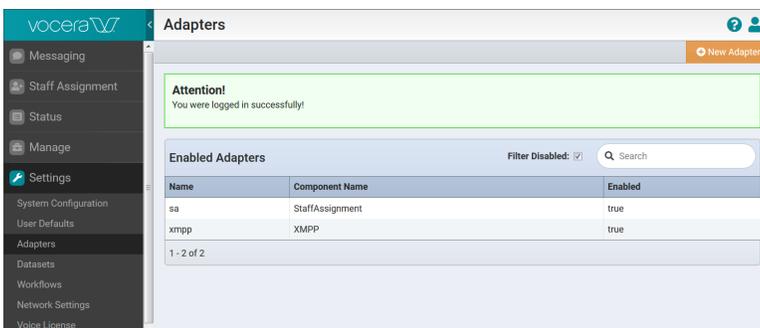
   The **Adapters** page displays.

3. Select an adapter to work with from the list displayed in the grid, or select the New Adapter Action option to create a new adapter.

   On the **Adapters** page you can identify adapters by their name or component name. The Enabled column (displaying a true or false status) indicates whether the adapter is active on the system, or disabled.

   The bottom row of the grid reports the number of adapters displayed, of the available adapters.

   The Filter Disabled box is checked by default, and displays only the enabled adapters that are configured on the Vocera Platform.
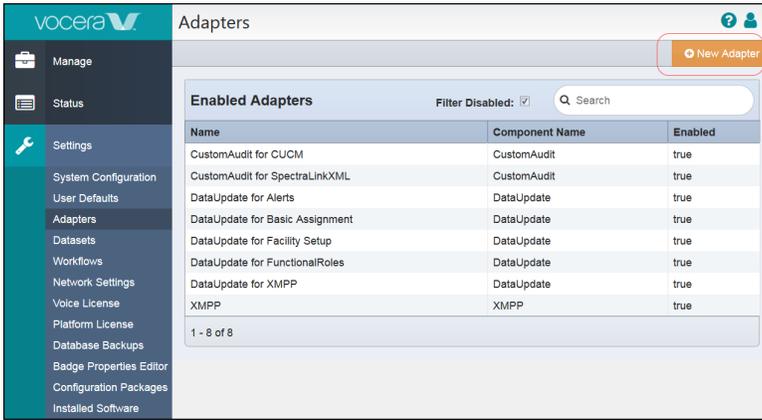
4. Uncheck the **Filter Disabled** box to display all the adapters that have been installed, including those that are not currently enabled. The column title now displays **All Adapters**.

The Filter Disabled box is checked by default.
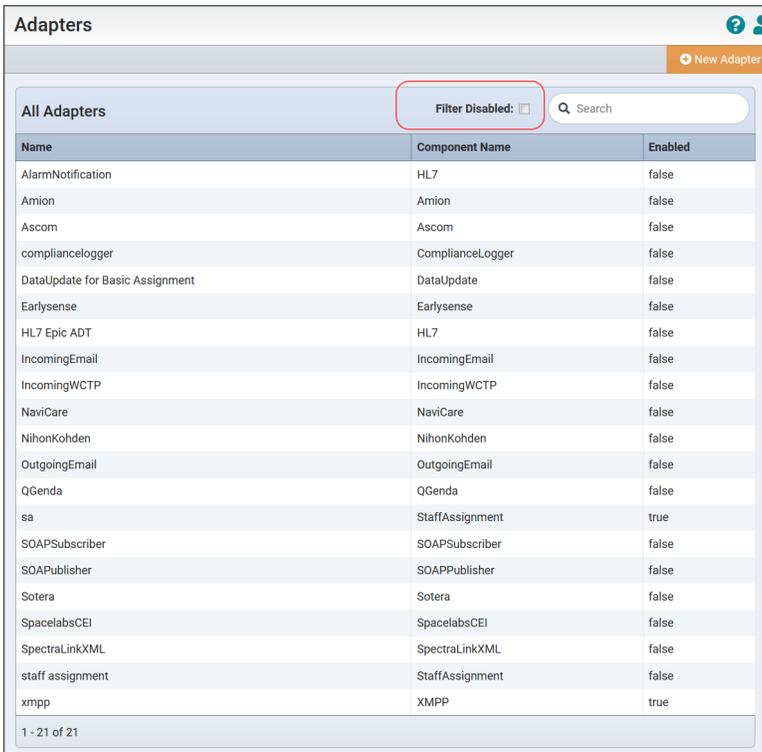
5. Enter a term in the **Search** field to locate a needed adapter on the system.

The search field is identified by a text field with a magnifying glass icon. The search is performed on the Name and Component Name columns.

When results are returned, the column header displays **Adapters Search Results** and an **x** icon allows you to clear the search field.
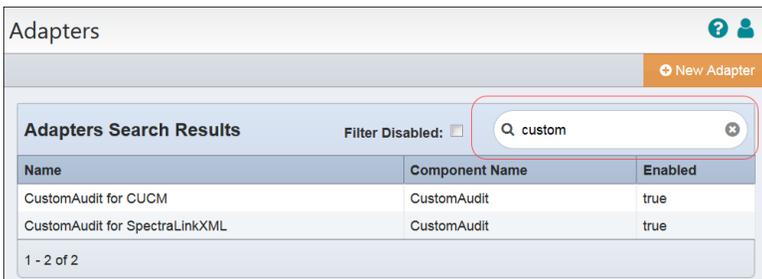
Editing an Adapter

Edit an adapter that has been installed on the Vocera Platform.

This page is used by all the adapter guides, and therefore, the adapter used as an example here may not be the adapter that you are working with currently.

1. Access the Vocera Platform Web Console and navigate to the adapters.

   See Navigating the Vocera Platform Adapters on page 96 for instructions.

2. Select the adapter to edit in the **Adapters** list.

3. Select **Edit** in the adapter's menu.

   The **Update Adapter** page for the adapter displays.

4. Edit the adapter's settings to revise the configuration as needed. See the adapter-specific configuration page for details on working with settings for this adapter.

   Select an empty field and begin typing, or select an existing value and type over it. To keep an existing value, do not edit that field.

5. Select one of the options to exit the **Update Adapter** page. See Saving an Adapter on page 100 for details.

Creating a New Adapter

Access the Vocera Platform Web Console to work with adapters, or create a new adapter when prompted in the package import process.

This page is used by all the adapter guides, and therefore, the adapter used as an example here may not be the adapter that you are working with currently.

1. Access the Vocera Platform Web Console and navigate to the adapters.

    See for instructions.

2. Select **New Adapter** in the Action menu on the Adapters page.
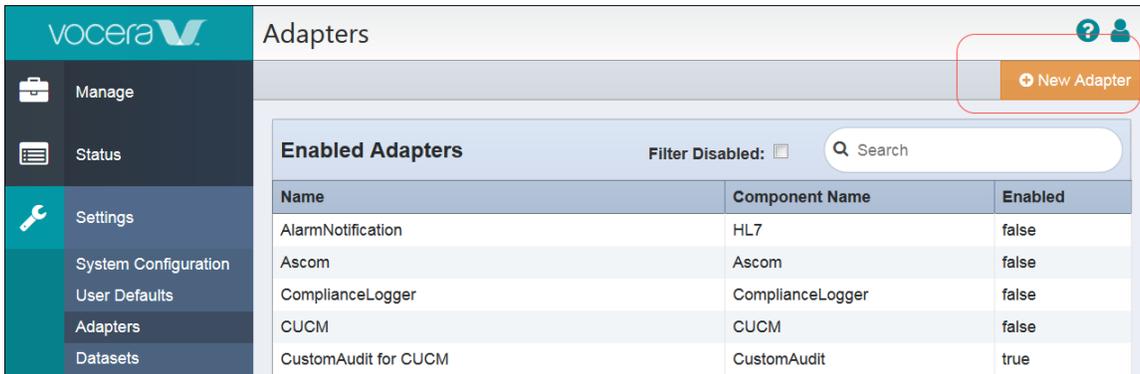
    The **Create a New Adapter** dialog displays.

3. Complete the configuration fields.
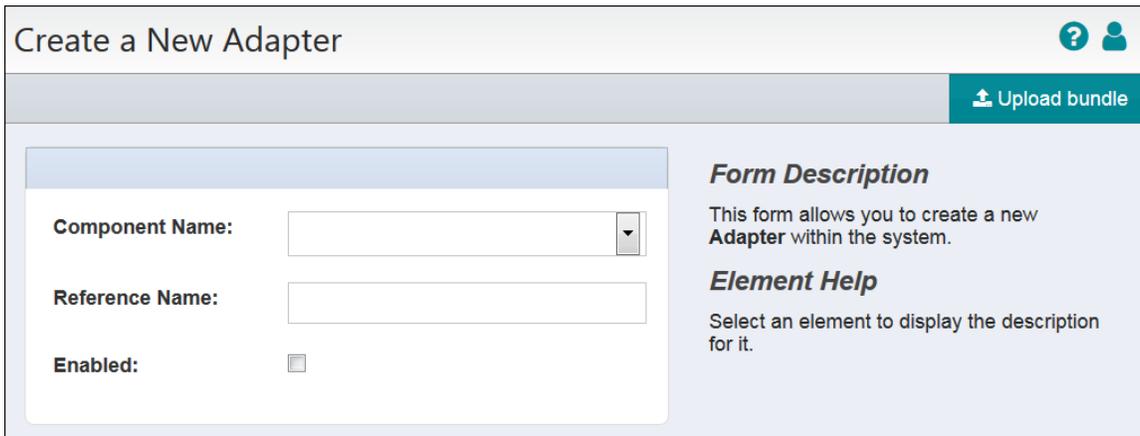
Name	Description
Component Name *	Select the Component Name field dropdown arrow to display a list of the systems and devices that Vocera currently supports. Select the name of the adapter to create.
Reference Name	Enter a short descriptive name in the Reference Name field to uniquely identify an adapter instance. It may demonstrate the adapter function or other information; for example, Production adapter may differentiate a live adapter from a development or "sandbox" adapter.
Enabled	Select the Enabled check box to allow Vocera Platform to use the new adapter. Vocera ignores the adapter if this option is disabled.

4. Select **Upload Bundle** in the Action menu to install a package on a Vocera Platform.

    Use the Upload Bundle feature to install when the adapter is not available in the Component Name dropdown list, and you have downloaded the needed adapter bundle to a storage location.

5. Click on **Browse** to navigate to the bundle to install.
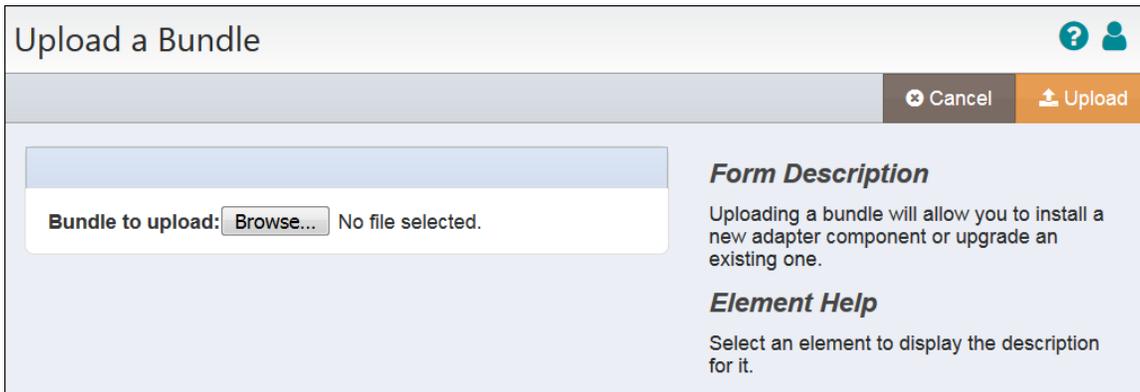
6. Select one of the Action options to exit from the Upload a Bundle dialog.
   - **Upload**: Upload the selected bundle to the appliance.
   - **Cancel**: Close the Upload a Bundle dialog without making a change to the system.

Saving an Adapter

Close an adapter configuration dialog using the Save, Reset, or Cancel options.

This page is used by all the adapter guides, and therefore, the adapter used as an example here may not be the adapter that you are working with currently.

When creating a new adapter, the options at the bottom of the adapter configuration page are Save, and Cancel.

When editing an existing adapter, the options are Save, Reset, and Cancel.

Choose an option to close the dialog:
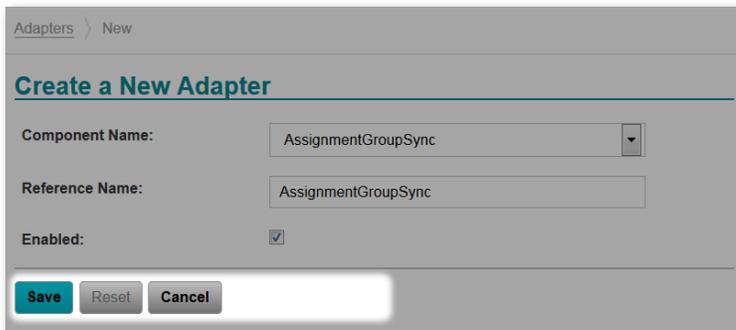
Option	Description
Save	Select Save to store the adapter configuration in the system, when the fields are set to desired specifications.
Cancel	Select Cancel to close the configuration window without saving your changes to the system.
Reset	Select Reset to clear all fields without closing the window, in order to select other specifications for the adapter's settings.

Deactivating an Adapter

Temporarily deactivate an adapter to avoid unintentional use of it in an implementation.

This page is used by all the adapter guides, and therefore, the adapter used as an example here may not be the adapter that you are working with currently.

1. Access the Vocera Platform Web Console and navigate to the adapter to deactivate.

   See Navigating the Vocera Platform Adapters on page 96 for instructions.

2. Select **Edit** in the Actions menu to access the Update page for the adapter.

3. Un-check the **Enabled** box to temporarily deactivate the adapter.

   When deactivated, the Vocera system will ignore the adapter. You can easily enable or disable the adapter at any time.

4. Select one of the options to exit the **Update Adapter** page. See Saving an Adapter on page 100 for details.

Removing an Adapter

Permanently remove an adapter from the Vocera system.

This page is used by all the adapter guides, and therefore, the adapter used as an example here may not be the adapter that you are working with currently.

Use the remove function to permanently delete the adapter from the system. Alternatively, you can disable an adapter and the Vocera system will ignore it.
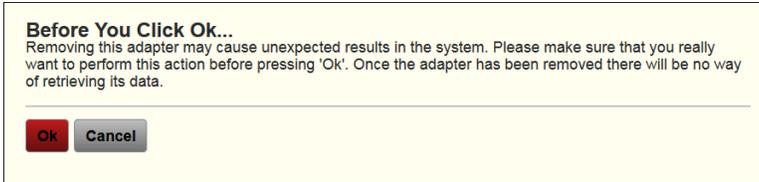
⚠️ **Warning:** Remove cannot be undone. If any system features use this adapter, removing the adapter prevents the features from functioning.

1. Access the Vocera Platform Web Console and navigate to the adapter to remove.

   See Navigating the Vocera Platform Adapters on page 96 for instructions.

2. Select **Remove** in the Actions menu to permanently delete the adapter.

3. Click **Ok** in the confirmation window.

Before You Click Ok...
Removing this adapter may cause unexpected results in the system. Please make sure that you really want to perform this action before pressing 'Ok'. Once the adapter has been removed there will be no way of retrieving its data.

Ok   Cancel

- **Ok**: Confirm the choice to remove the adapter from the system.
- **Cancel**: Return to the adapter page without making a change.

4. Confirm that the adapter no longer displays in the Adapters list view, when a success message displays.

Adapters   ❓ 👤

⊕ New Adapter

Attention!
The adapter was removed from the system successfully.