Unified Communications Mobile and Remote Access via Cisco VCS

Deployment Guide

Cisco VCS X8.2
Cisco Unified CM 9.1(2)SU1 or later

January 2015

Contents

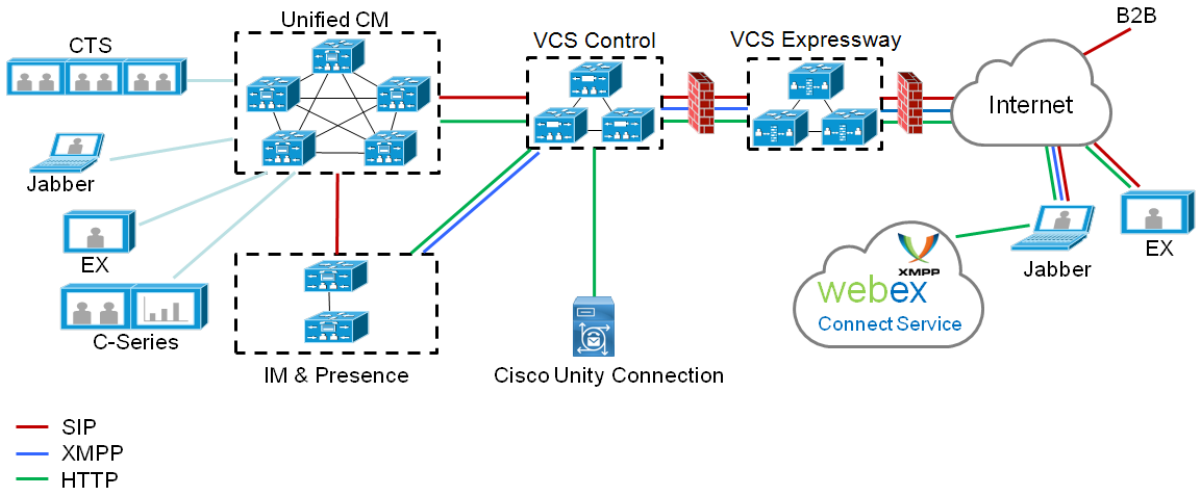
Mobile and remote access overview

Cisco Unified Communications mobile and remote access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is not within the enterprise network. The VCS provides secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides:

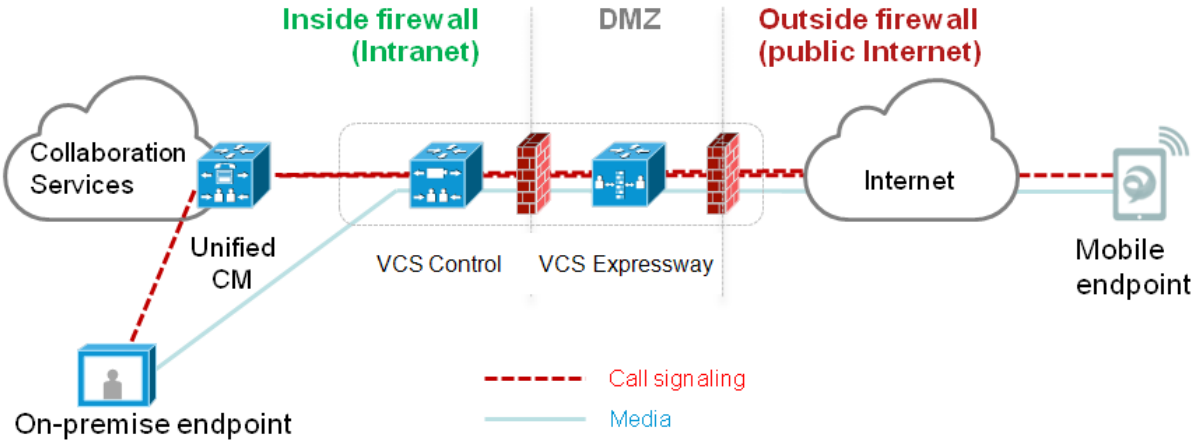
- **Off-premises access**: a consistent experience outside the network for Jabber and EX/MX/SX Series clients
- **Security**: secure business-to-business communications
- **Cloud services**: enterprise grade flexibility and scalable solutions providing rich WebEx integration and Service Provider offerings
- **Gateway and interoperability services**: media and signaling normalization, and support for non-standard endpoints

Figure 1: Unified Communications: mobile and remote access



Note that third-party SIP or H.323 devices can register to the VCS Control and, if necessary, interoperate with Unified CM-registered devices over a SIP trunk.

Figure 2: Typical call flow: signaling and media paths



- Unified CM provides call control for both mobile and on-premises endpoints.
- Signaling traverses the Expressway solution between the mobile endpoint and Unified CM.
- Media traverses the Expressway solution and is relayed between endpoints directly; all media is encrypted between the VCS Control and the mobile endpoint.

Jabber client connectivity without VPN

The mobile and remote access solution supports a hybrid on-premises and cloud-based service model, providing a consistent experience inside and outside the enterprise. It provides a secure connection for Jabber application traffic without having to connect to the corporate network over a VPN. It is a device and operating system agnostic solution for Cisco Unified Client Services Framework clients on Windows, Mac, iOS and Android platforms.

It allows Jabber clients that are outside the enterprise to:

- use instant messaging and presence services
- make voice and video calls
- search the corporate directory
- share content
- launch a web conference
- access visual voicemail

Note that Jabber Web and Cisco Jabber Video for TelePresence (Jabber Video) are not supported.

Related documentation

Information contained in the following documents and sites may be required to assist in setting up your Unified Communications environment:

- *VCS Basic Configuration (Control with Expressway) Deployment Guide*
- *VCS Cluster Creation and Maintenance Deployment Guide*
- *Certificate Creation and Use With VCS Deployment Guide*
- *VCS Administrator Guide*

- *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager Communications Manager*
- Jabber client configuration details:
  - *Cisco Jabber for Windows*
  - *Cisco Jabber for iPad*
  - *Cisco Jabber for Android*
  - *Cisco Jabber DNS Configuration Guide*

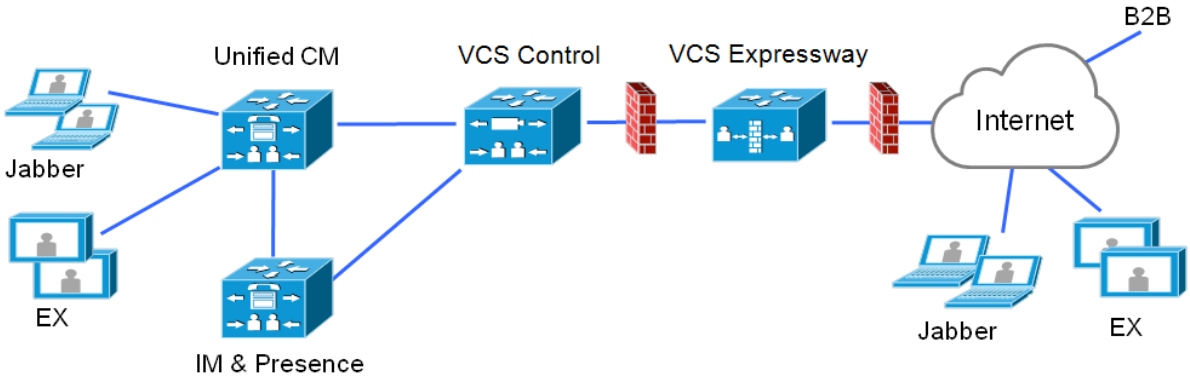
Deployment scenarios

This section describes the supported deployment environments:

- single network elements
- single clustered network elements
- multiple clustered network elements
- hybrid deployment

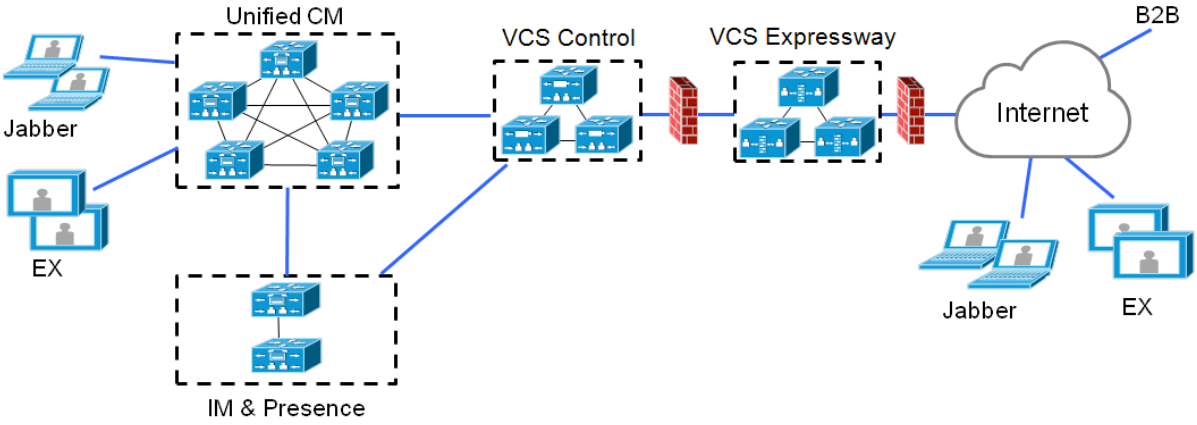
Single network elements

In this scenario there are single (non-clustered) Unified CM, IM & Presence, VCS Control and VCS Expressway servers.



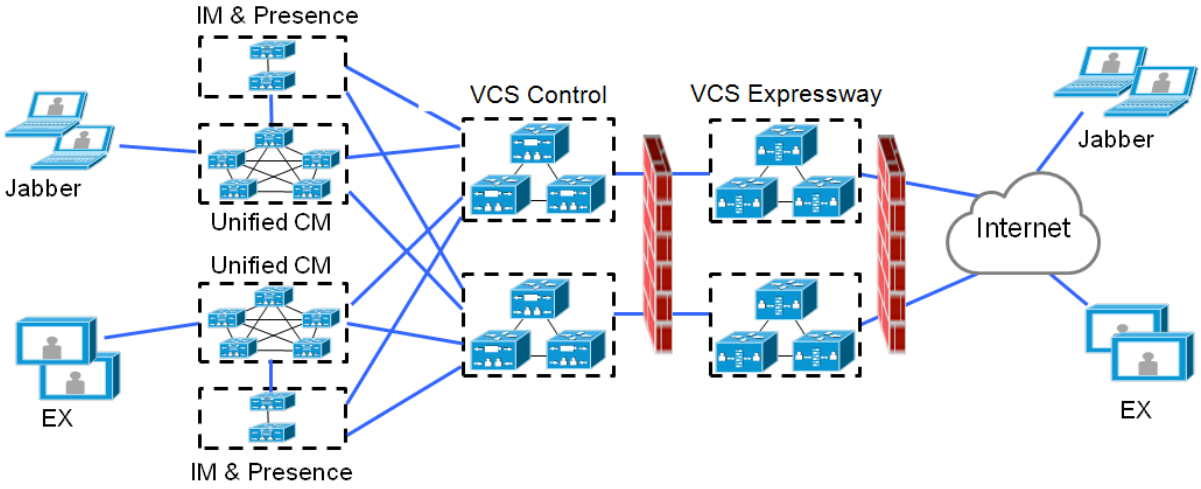
Single clustered network elements

In this scenario each network element is clustered.



Multiple clustered network elements

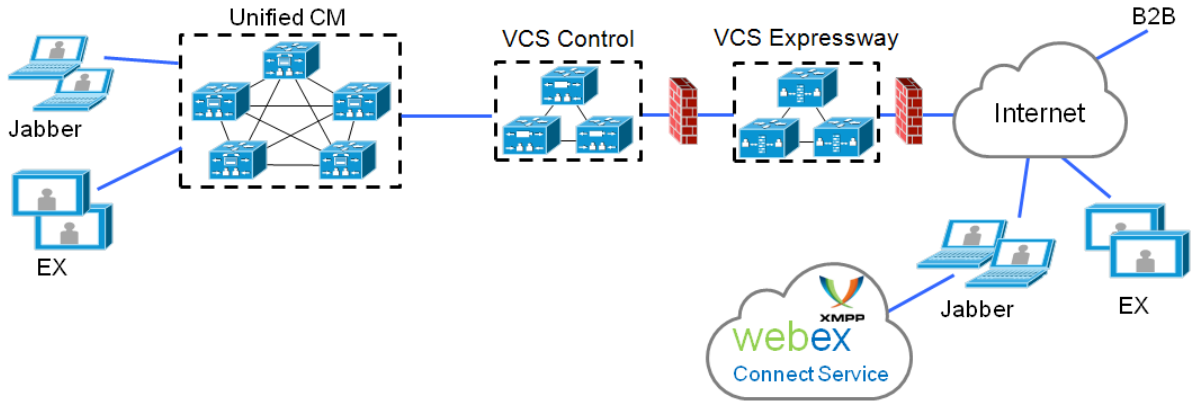
In this scenario there are multiple clusters of each network element.



Jabber clients can access their own cluster via any route. Each Unified CM and IM & Presence cluster combination must use the same domain.

Hybrid deployment

In this scenario, IM and Presence services for Jabber clients are provided via the WebEx cloud.



Configuration overview

This section summarizes the steps involved in configuring your Unified Communications system for mobile and remote access. It assumes that you already have set up:

- a basic VCS Control and VCS Expressway configuration as specified in *VCS Basic Configuration (Control with Expressway) Deployment Guide* (this document contains information about the different networking options for deploying the VCS Expressway in the DMZ)
- Unified CM and IM and Presence Servers have been configured as specified in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* (for your version), at Cisco Unified Communications Manager Configuration Guides

Prerequisites

Ensure that you are running the following software versions:

- VCS X8.1.1 or later
- Unified CM 9.1(2)SU1 or later and IM and Presence Servers 9.1(1) or later

Supported clients when using mobile and remote access

- Cisco Jabber for Windows 9.7 or later
- Cisco Jabber for iOS (iPhone and iPad) 9.6.1 or later
- Cisco Jabber for Android 9.6 or later
- Cisco TelePresence endpoints/codecs running TC7.0.1 or later firmware

Configuration summary

EX/MX/SX Series endpoints (running TC software)

Ensure that the provisioning mode is set to *Cisco UCM via Expressway*.

On Unified CM, you need to ensure that the **IP Addressing Mode** for these endpoints is set to *IPV4_ONLY*.

These endpoints must verify the identity of the VCS Expressway they are connecting to by validating its server certificate. To do this, they must have the certificate authority that was used to sign the VCS Expressway's server certificate in their list of trusted CAs.

These endpoints ship with a list of default CAs which cover the most common providers (Verisign, Thawte, etc). If the relevant CA is not included, it must be added. See 'Managing the list of trusted certificate authorities' in the endpoint's administrator guide.

Mutual authentication is optional; these endpoints are not required to provide client certificates. If you do want to configure mutual TLS, you cannot use CAPF enrolment to provision the client certificates; you must manually apply the certificates to the endpoints. The client certificates must be signed by an authority that is trusted by the VCS Expressway.

Jabber clients

Jabber clients must verify the identity of the VCS Expressway they are connecting to by validating its server certificate. To do this, they must have the certificate authority that was used to sign the VCS Expressway's

server certificate in their list of trusted CAs.

Jabber uses the underlying operating system's certificate mechanism:

- Windows: Certificate Manager
- MAC OS X: Key chain access
- IOS: Trust store
- Android: Location & Security settings

Jabber client configuration details for mobile and remote access is contained within the relevant installation and configuration for that Jabber client:

- *Cisco Jabber for Windows*
- *Cisco Jabber for iPad*
- *Cisco Jabber for Android*
- *Cisco Jabber for Mac* (requires X8.2 or later)

DNS records

This section summarizes the public (external) and local (internal) DNS requirements. For more information, see *Cisco Jabber DNS Configuration Guide*.

Public DNS

The public (external) DNS must be configured with **`_collab-edge._tls.<domain>`** SRV records so that endpoints can discover the VCS Expressways to use for mobile and remote access. SIP service records are also required (for general deployment, not specifically for mobile and remote access). For example, for a cluster of 2 VCS Expressway systems:

Domain	Service	Protocol	Priority	Weight	Port	Target host
example.com	collab-edge	tls	10	10	8443	vcse1.example.com
example.com	collab-edge	tls	10	10	8443	vcse2.example.com
example.com	sips	tcp	10	10	5061	vcse1.example.com
example.com	sips	tcp	10	10	5061	vcse2.example.com

Local DNS

The local (internal) DNS requires **`_cisco-uds._tcp.<domain>`** and **`_cuplogin._tcp.<domain>`** SRV records. For example:

Domain	Service	Protocol	Priority	Weight	Port	Target host
example.com	cisco-uds	tcp	10	10	8443	cucmserver.example.com
example.com	cuplogin	tcp	10	10	8443	cupserver.example.com

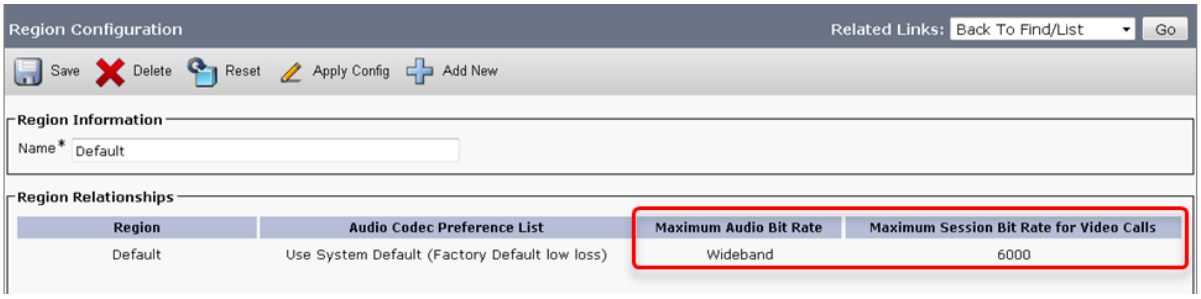
Ensure that the **`cisco-uds`** and **`_cuplogin`** SRV records are NOT resolvable outside of the internal network, otherwise the Jabber client will not start mobile and remote access negotiation via the VCS Expressway.

Firewall

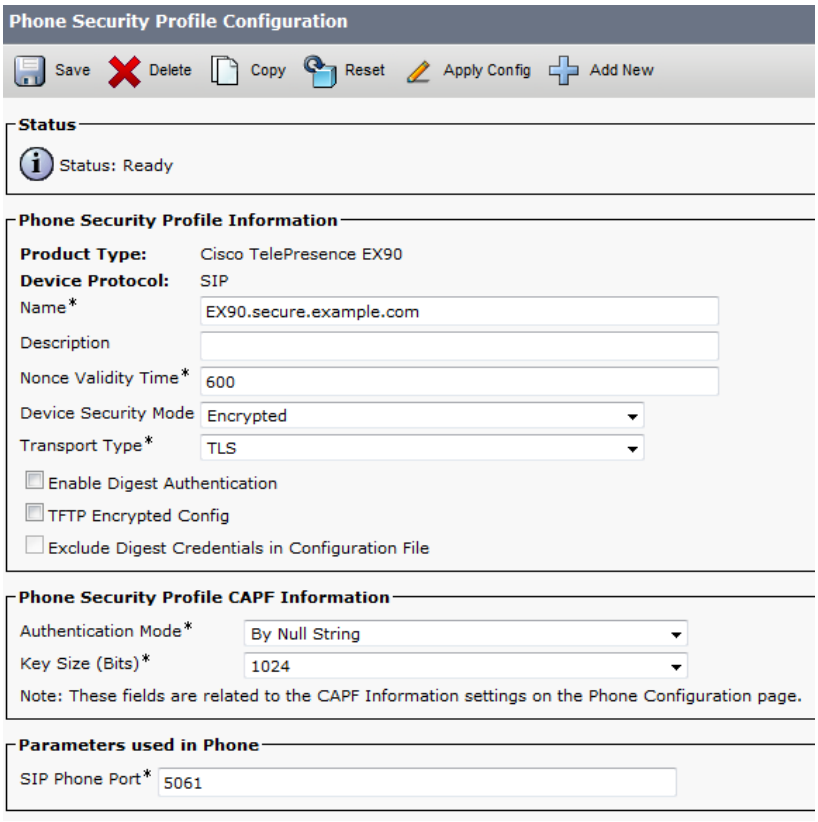
- Ensure that the relevant ports have been configured on your firewalls between your internal network (where the VCS Control is located) and the DMZ (where the VCS Expressway is located) and between the DMZ and the public internet. See Mobile and remote access port reference [p.27] for more information.
- If your VCS Expressway has one NIC enabled and is using static NAT mode, note that:
  You must enter the FQDN of the VCS Expressway, as it is seen from outside the network, as the peer address on the VCS Control's secure traversal zone. The reason for this is that in static NAT mode, the VCS Expressway requests that incoming signaling and media traffic should be sent to its external FQDN, rather than its private name.
  This also means that the external firewall must allow traffic from the VCS Control to the VCS Expressway's external FQDN. This is known as NAT reflection, and may not be supported by all types of firewalls.
  See the *Advanced network deployments* appendix, in the *VCS Basic Configuration (Control with Expressway) Deployment Guide*, for more information.

Unified CM

1. If you have multiple Unified CM clusters, you must confgure ILS (Intercluster Lookup Service) on all of the clusters.
   This is because the VCS needs to communicate with each user's home Unified CM cluster, and to discover the home cluster it sends a UDS (User Data Service) query to any one of the Unified CM nodes. Search for "Intercluster Lookup Service" in the Unified CM documentation for your version.
2. Ensure that the **Maximum Session Bit Rate for Video Calls** between and within regions (**System > Region Information > Region**) is set to a suitable upper limit for your system, for example 6000 kbps.



   See *Region setup* for more information.
3. The **Phone Security Profiles** in Unified CM (**System > Security > Phone Security Profile**) that are configured for TLS and are used for devices requiring remote access must have a **Name** in the form of an FQDN that includes the enterprise domain, for example jabber.secure.example.com. (This is because those names must be present in the list of Subject Alternate Names in the VCS Control's server certificate.)



4. If Unified CM servers (**System > Server**) are configured by **Host Name** (rather than IP address), then ensure that those host names are resolvable by the VCS Control.
5. If you are using secure profiles, ensure that the root CA of the authority that signed the VCS Control certificate is installed as a *CallManager-trust* certificate (**Security > Certificate Management** in the **Cisco Unified OS Administration** application).
6. Ensure that the **Cisco AXL Web Service** is active on the Unified CM publishers you will be using to discover the Unified CM servers that are to be used for remote access. To check this, select the **Cisco Unified Serviceability** application and go to **Tools > Service Activation**.
7. We recommend that remote and mobile devices are configured (either directly or by Device Mobility) to use publicly accessible NTP servers.
   a. Configure a public NTP server **System > Phone NTP Reference**.
   b. Add the Phone NTP Reference to a Date/Time Group (**System > Date/Time Group**).
   c. Assign the Date/Time Group to the Device Pool of the endpoint (**System > Device Pool**).

IM and Presence Service

Ensure that the **Cisco AXL Web Service** is active on the IM and Presence Service publishers that will discover other IM and Presence Servers nodes for remote access. To check this, select the **Cisco Unified Serviceability** application and go to **Tools > Service Activation**.

If you are deploying Mobile and Remote Access with multiple IM and Presence Servers clusters, you must configure Intercluster peer links between the clusters, and the Intercluster Sync Agent (ICSA) must be active on all clusters. This ensures that the user database is replicated between clusters, allowing VCS Control to correctly route XMPP traffic.

For details of the correct configuration, refer to the chapter "Intercluster Peer Configuration" in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*. You can find the

correct document for your version at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

VCS

The following steps summarize the configuration required on the VCS Expressway and the VCS Control. Full details are described in section Configuring mobile and remote access on VCS [p.14]

1. Ensure that **System host name** and **Domain name** are specified for every VCS, and that all VCS systems are synchronized to a reliable NTP service.
2. Set **Unified Communications mode** to *Mobile and remote access*.
3. Configure the Unified CM, IM and Presence Servers, and Cisco Unity Connection servers on the VCS Control.
4. Configure the domains on the VCS Control for which services are to be routed to Unified CM.
5. Install appropriate server certificates and trusted CA certificates.
6. Configure a Unified Communications traversal zone connection between the VCS Expressway and the VCS Control.
7. If required, configure the HTTP server allow list (whitelist) for any web services inside the enterprise that need to be accessed from remote Jabber clients.

Note that configuration changes on the VCS generally take immediate effect. If a system restart or other action is required you will be notified of this either through a banner message or via an alarm.

Configuring mobile and remote access on VCS

This section describes the steps required to enable and configure mobile and remote access features on VCS Control and VCS Expressway, and how to discover the Unified CM servers and IM&P servers used by the service.

Installing VCS security certificates and setting up a secure traversal zone

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be a secure traversal zone connection between the VCS Control and the VCS Expressway. This involves:

- Installing suitable security certificates on the VCS Control and the VCS Expressway.
- Configuring an encrypted traversal zone between the VCS Control and the VCS Expressway

For information about how to do this, see:

- Configuring a secure traversal zone connection for Unified Communications [p.21] (if your system does not already have a secure traversal zone in place)
- Server certificate requirements for Unified Communications [p.24]

Note that if XMPP federation is to be used, the IM&P servers need to be discovered on the VCS Control for all the relevant information to be available when generating certificate signing requests.

Setting up the VCS Control

This section describes the configuration steps required on the VCS Control.

Configuring DNS and NTP settings

Check and configure the basic system settings on VCS:

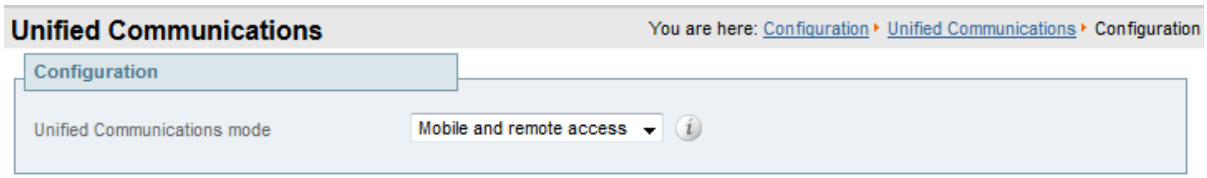
1. Ensure that **System host name** and **Domain name** are specified (**System > DNS**).
2. Ensure that local DNS servers are specified (**System > DNS**).
3. Ensure that all VCS systems are synchronized to a reliable NTP service (**System > Time**). Use an **Authentication** method in accordance with your local policy.

If you have a cluster of VCSs you must do this for every peer.

Enabling the VCS Control for mobile and remote access

To enable mobile and remote access functionality:

1. Go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Mobile and remote access*.
3. Click **Save**.



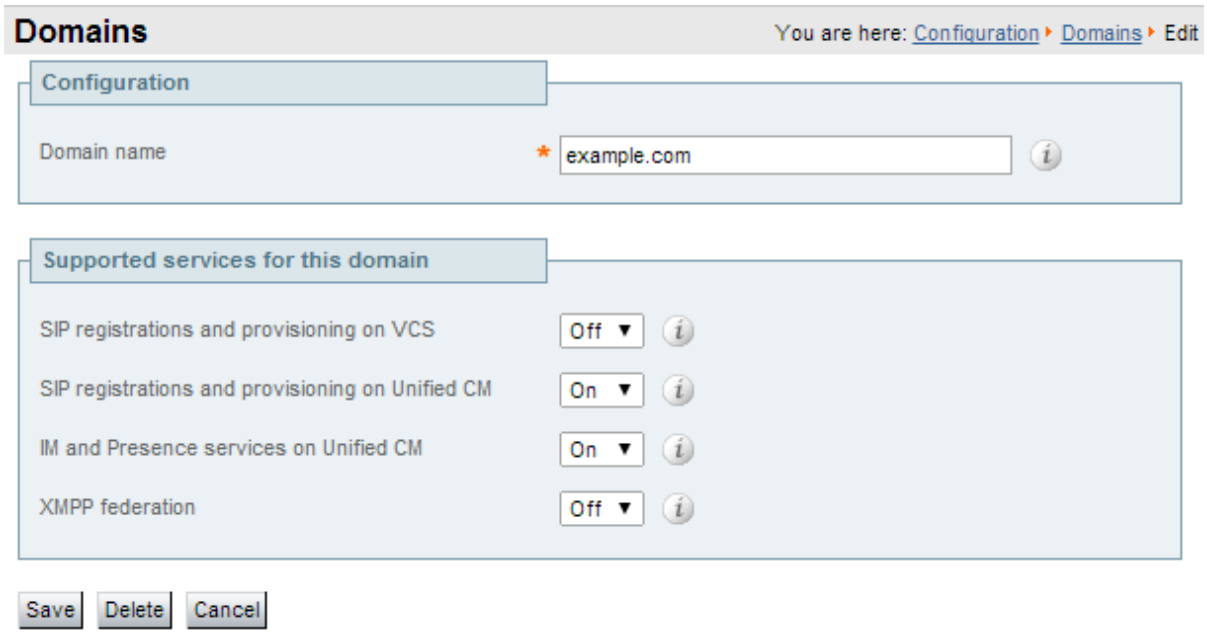
Note that you must select *Mobile and remote access* before you can configure the relevant domains and traversal zones.

Configuring the domains to route to Unified CM

You must configure the domains for which registration, call control, provisioning, messaging and presence services are to be routed to Unified CM.

1. On VCS Control, go to **Configuration > Domains**.
2. Select the domains (or create a new domain, if not already configured) for which services are to be routed to Unified CM.
3. For each domain, turn *On* the services for that domain that VCS is to support. The available services are:
   - **SIP registrations and provisioning on VCS**: the VCS is authoritative for this SIP domain. The VCS acts as a SIP registrar and Presence Server for the domain, and accepts registration requests for any SIP endpoints attempting to register with an alias that includes this domain.
   - **SIP registrations and provisioning on Unified CM**: endpoint registration, call control and provisioning for this SIP domain is serviced by Unified CM. The VCS acts as a Unified Communications gateway to provide secure firewall traversal and line-side support for Unified CM registrations.
   - **IM and Presence services on Unified CM**: instant messaging and presence services for this SIP domain are provided by the Unified CM IM and Presence service.
   - **XMPP federation**: enables XMPP federation between this domain and partner domains.

   Turn *On* all of the applicable services for each domain. For example, the same domain may be used by endpoints such as Jabber or EX Series devices that require line-side Unified Communications support, and by other endpoints such as third-party SIP or H.323 devices that require VCS support. (In this scenario, the signaling messages sent from the endpoint indicate whether line-side unified communications or VCS support is required.)



Discovering Unified Communications servers and services

The VCS Control must be configured with the address details of the Unified Communications services/nodes that are going to provide registration, call control, provisioning, voicemail, messaging, and presence services to MRA users.

IM and Presence Servers configuration is not required if you're deploying the hybrid model, as these services are provided by the WebEx cloud.

Note: The connections configured in this procedure are static. You must refresh the configuration on the VCS Control after you reconfigure or upgrade any of the discovered Unified Communications nodes.

Go to **Configuration > Unified Communications > *<UC server type>*** and click **Refresh servers**.

Trusting the certificates presented to the VCS Control

If **TLS verify mode** is *On* when discovering Unified Communications services, then you must configure the VCS Control to trust the certificates presented by the IM and Presence Servers and Unified CM servers.

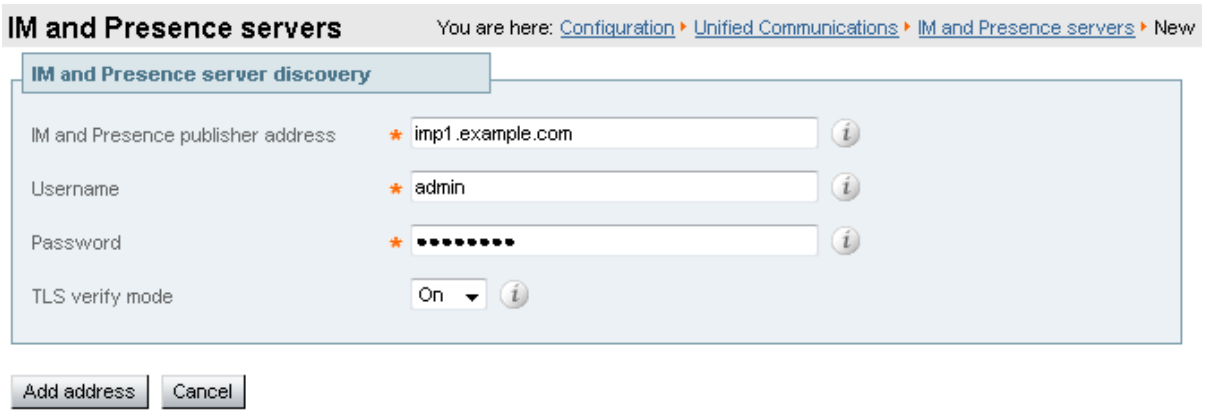
1. Determine the relevant CA certificates to upload:
   - If the servers' tomcat and CallManager certificates are CA-signed, the VCS Control's trusted CA list must include the root CA of the certificate issuer.
   - If the servers are using self-signed certificates, the VCS Control's trusted CA list must include the self-signed certificates from all discovered IM and Presence Servers nodes, Cisco Unity Connection servers, and Unified CM servers.
2. Upload the required certificates to the VCS Control (**Maintenance > Security certificates > Trusted CA certificate**).
3. Restart the VCS Control (**Maintenance > Restart options**).

Discovering IM and Presence Servers

1. On VCS Control, go to **Configuration > Unified Communications > IM and Presence Servers**.
   The page lists any IM and Presence Servers that have already been discovered.
2. Add the details of an IM and Presence Servers database publisher node:
   a. Click **New**.
   b. Enter the address of the **IM and Presence Servers database publisher node**.
   You can enter an FQDN or an IP address, but we recommend using the FQDN when **TLS verify mode** is *On*.
   c. Enter the **Username** and **Password** of an account that can access this server.

   Note: These credentials are stored permanently in the VCS database. The corresponding IM and Presence Servers user must have the *Standard AXL API Access* role.

   d. [Recommended] Leave **TLS verify mode** switched *On* to ensure VCS verifies the node's tomcat certificate (for XMPP-related communications).
   e. Click **Add address**.
   The system attempts to contact the publisher and retrieve details of its associated nodes.



   Note: The status of the discovered node will be **Inactive** unless a valid traversal zone connection exists between the VCS Control and the VCS Expressway (may not yet be configured).

3. Repeat the discovery procedure for other IM and Presence Servers nodes/clusters, if required.
4. Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

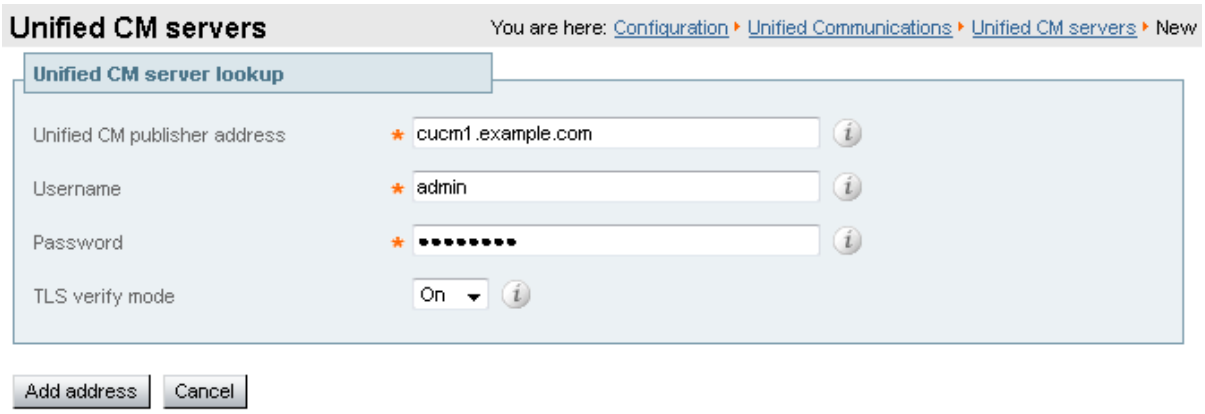
Discovering Unified CM servers

1. On VCS Control, go to **Configuration > Unified Communications > Unified CM servers**.
   The page lists any Unified CM nodes that have already been discovered.
2. Add the details of a Unified CM publisher node:
   a. Click **New**.
   b. Enter the **Unified CM publisher address**.
   You can enter an FQDN or an IP address, but we recommend using the FQDN when **TLS verify mode** is *On*.
   c. Enter the **Username** and **Password** of an account that can access this server.

Note: These credentials are stored permanently in the VCS database. The corresponding Unified CM user must have the *Standard AXL API Access* role.

d. [Recommended] Leave **TLS verify mode** switched *On* to ensure VCS verifies the node's certificates. The Unified CM node presents its tomcat certificate for AXL and UDS queries, and its CallManager certificate for subsequent SIP traffic. If the Unified CM server is using self-signed certificates, the VCS Control's trusted CA list must include a copy of the tomcat certificate and the CallManager certificate from every Unified CM server.

e. Click **Add address**.
The system attempts to contact the publisher and retrieve details of its associated nodes.



3. Repeat the discovery procedure for other Unified CM nodes/clusters, if required.
4. Click **Refresh servers** to refresh all the node details after configuring multiple publisher addresses.

Automatically generated zones and search rules

VCS Control automatically generates non-configurable neighbor zones between itself and each discovered Unified CM node. A TCP zone is always created, and a TLS zone is created also if the Unified CM node is configured with a **Cluster Security Mode** (**System > Enterprise Parameters > Security Parameters**) of *1 (Mixed)* (so that it can support devices provisioned with secure profiles). The TLS zone is configured with its **TLS verify mode** set to *On* if the Unified CM discovery had **TLS verify mode** enabled. This means that the VCS Control will verify the CallManager certificate for subsequent SIP communications. Each zone is created with a name in the format 'CEtcp-<node name>' or 'CEtls-<node name>'.

A non-configurable search rule, following the same naming convention, is also created automatically for each zone. The rules are created with a priority of 45. If the Unified CM node that is targeted by the search rule has a long name, the search rule will use a regex for its address pattern match.

Note that load balancing is managed by Unified CM when it passes routing information back to the registering endpoints.

Configuring the HTTP server allow list (whitelist) on VCS Control

Jabber client endpoints may need to access additional web services inside the enterprise. This requires an "allow list" of servers to be configured to which the VCS will grant access for HTTP traffic originating from outside the enterprise.

The features and services that may be required, and would need whitelisting, include:

- Visual Voicemail
- Jabber Update Server
- Custom HTML tabs / icons
- Directory Photo Host

To configure the set of addresses to which HTTP access will be allowed:

1. On VCS Control, go to **Configuration > Unified Communications > Configuration**.
2. Click **HTTP server allow list**.
3. Configure the hostnames or IP addresses of an HTTP server that a Jabber client located outside of the enterprise is allowed to access.
   Access is granted if the server portion of the client-supplied URI matches one of the names entered here, or if it resolves via DNS lookup to a specified IP address.

The IP addresses of all discovered Unified CM nodes (that are running the CallManager or TFTP service) and IM&P nodes are added automatically to the allow list and cannot be deleted. These addresses are displayed in the **Auto-configured allow list** section of the **HTTP server allow list** page.

Setting up the VCS Expressway

This section describes the configuration steps required on the VCS Expressway.

Configuring DNS and NTP settings

Check and configure the basic system settings on VCS:

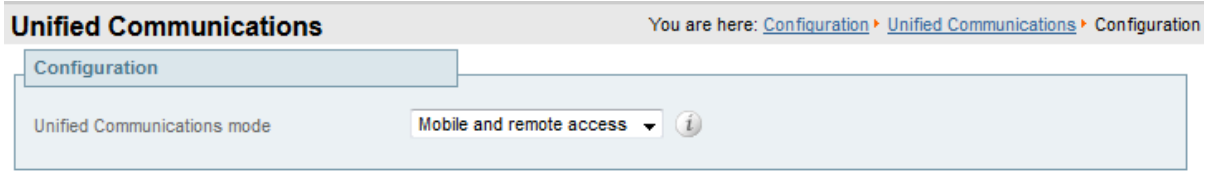
1. Ensure that **System host name** and **Domain name** are specified (**System > DNS**).
   Note that <**System host name**>.<**Domain name**> is the FQDN of this VCS Expressway. Ensure that this FQDN is resolvable in public DNS.
2. Ensure that public DNS servers are specified (**System > DNS**).
3. Ensure that all VCS systems are synchronized to a reliable NTP service (**System > Time**). Use an **Authentication** method in accordance with your local policy.

If you have a cluster of VCSs you must do this for every peer.

Enabling the VCS Expressway for mobile and remote access

To enable mobile and remote access functionality:

1. Go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Mobile and remote access*.
3. Click **Save**.



Ensuring that TURN services are disabled on VCS Expressway

You must ensure that TURN services are disabled on the VCS Expressway used for mobile and remote access.

1. Go to **Configuration > Traversal > TURN**.
2. Ensure that **TURN services** are *Off*.

Checking the status of Unified Communications services

You can check the status of the Unified Communications services on both VCS Control and VCS Expressway.

1. Go to **Status > Unified Communications**.
2. Review the list and status of domains, zones and (VCS Control only) Unified CM and IM&P servers. Any configuration errors will be listed along with links to the relevant configuration page from where you can address the issue.

Configuring a secure traversal zone connection for Unified Communications

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be a secure traversal zone connection between the VCS Control and the VCS Expressway. This involves:

- Installing suitable security certificates on the VCS Control and the VCS Expressway.
- Configuring an encrypted traversal zone between the VCS Control and the VCS Expressway

Installing VCS security certificates

You must set up trust between the VCS Control and the VCS Expressway:

1. Install a suitable server certificate on both the VCS Control and the VCS Expressway.
   - The certificate must include the **Client Authentication** extension. The system will not allow you to upload a server certificate without this extension when Unified Communications features have been enabled.
   - The VCS includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR:
     - Ensure that the CA that signs the request does not strip out the client authentication extension.
     - The generated CSR includes the client authentication request and any relevant subject alternate names for the Unified Communications features that have been enabled (see Server certificate requirements for Unified Communications [p.24] if appropriate).
   - To generate a CSR and /or to upload a server certificate to the VCS, go to **Maintenance > Security certificates > Server certificate**. You must restart the VCS for the new server certificate to take effect.
2. Install on both VCSs the trusted Certificate Authority (CA) certificates of the authority that signed the VCS's server certificates.
   There are additional trust requirements, depending on the Unified Communications features being deployed.
   For mobile and remote access deployments:
   - The VCS Control must trust the Unified CM and IM&P tomcat certificate.
   - If appropriate, both the VCS Control and the VCS Expressway must trust the authority that signed the endpoints' certificates.

   For Jabber Guest deployments:
   - When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the VCS Control either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server's certificate.

   To upload trusted Certificate Authority (CA) certificates to the VCS, go to **Maintenance > Security certificates > Trusted CA certificate**. You must restart the VCS for the new trusted CA certificate to take effect.

See *Certificate Creation and Use With VCS Deployment Guide* for full information about how to create and upload the VCS's server certificate and how to upload a list of trusted certificate authorities.

Configuring encrypted VCS traversal zones

To support Unified Communications features via a secure traversal zone connection between the VCS Control and the VCS Expressway:

- The VCS Control and VCS Expressway must be configured with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on a VCS Control, or a traversal server zone when selected on a VCS-E) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.
- Both VCSs must trust each other's server certificate. As each VCS acts both as a client and as a server you must ensure that each VCS's certificate is valid both as a client and as a server.
- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

To set up a secure traversal zone, configure your VCS Control and VCS Expressway as follows:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

	VCS Control	VCS Expressway
Name	"Traversal zone" for example	"Traversal zone" for example
Type	*Unified Communications traversal*	*Unified Communications traversal*
Connection credentials section		
Username	"exampleauth" for example	"exampleauth" for example
Password	"ex4mpl3.c0m" for example	Click **Add/Edit local authentication database**, then in the popup dialog click **New** and enter the **Name** ("exampleauth") and **Password** ("ex4mpl3.c0m") and click **Create credential**.
SIP section		
Port	`7001`	`7001`
TLS verify subject name	Not applicable	Enter the name to look for in the traversal client's certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate.
Authentication section		
Authentication policy	*Do not check credentials*	*Do not check credentials*
Location section		

	VCS Control	VCS Expressway
Peer 1 address	Enter the FQDN of the VCS Expressway. Note that if you use an IP address (not recommended), that address must be present in the VCS Expressway server certificate.	Not applicable
Peer 2...6 address	Enter the FQDNs of additional peers if it is a cluster of VCS Expressways.	Not applicable

Note that you should configure only one *Unified Communications traversal* zone per VCS.

4. Click **Create zone**.

Server certificate requirements for Unified Communications

The VCS certificate signing request (CSR) tool prompts for and incorporates the relevant subject alternate name (SAN) entries as appropriate for the Unified Communications features that are supported on that VCS.

The following table shows which CSR alternative name elements apply to which Unified Communications features:

CSR SAN element	Mobile and remote access	Jabber Guest	XMPP federation
Unified CM registrations domains	✓ (VCS Expressway only)	X	X
XMPP federation domains	X	X	✓ (VCS Expressway only)
IM and Presence chat node aliases (federated group chat)	X	X	✓
Unified CM phone security profile names	✓ (VCS Control only)	X	X

Note that:

- A new VCS Control certificate may need to be produced for the VCS Control if chat node aliases are added or renamed, such as when an IM and Presence node is added or renamed, or if new TLS phone security profiles are added.
- A new VCS Expressway certificate must be produced if new chat node aliases are added to the system, or if the Unified CM or XMPP federation domains are modified.
- You must restart the VCS for any new uploaded server certificate to take effect.

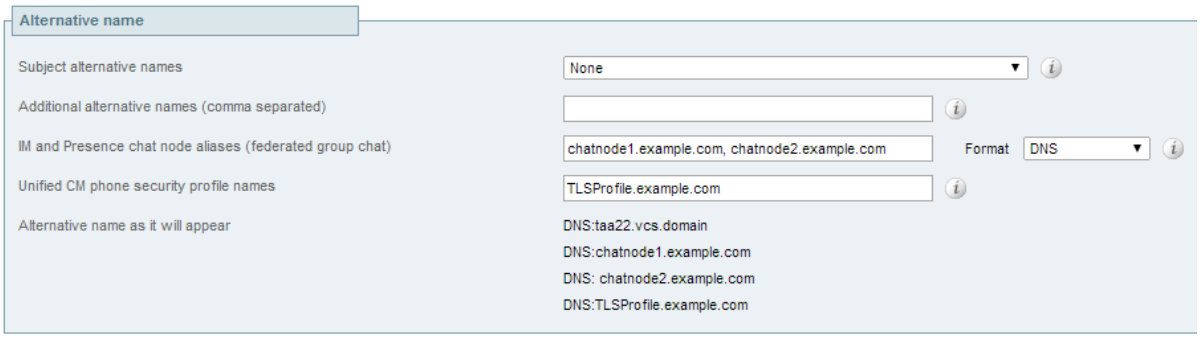
More details about the individual feature requirements per VCS Control / VCS Expressway are described below.

VCS Control server certificate requirements

The VCS Control server certificate needs to include the following elements in its list of subject alternate names:

- **Unified CM phone security profile names**: the names, in FQDN format, of all of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. This ensures that Unified CM can communicate with VCS Control via a TLS connection when it is forwarding messages from devices that are configured with those security profiles.
- **IM and Presence chat node aliases (federated group chat)**: the **Chat Node Aliases** (e.g. chatroom1.example.com) that are configured on the IM and Presence servers. These are required only for Unified Communications XMPP federation deployments that intend to support group chat over TLS with federated contacts.
  The VCS Control automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM&P servers.
  We recommend that you use DNS format for the chat node aliases when generating the CSR. You must include the same chat node aliases in the VCS Expressway server certificate's alternative names.

Figure 3: Entering subject alternative names for security profiles and chat node aliases on the VCS Control's CSR generator

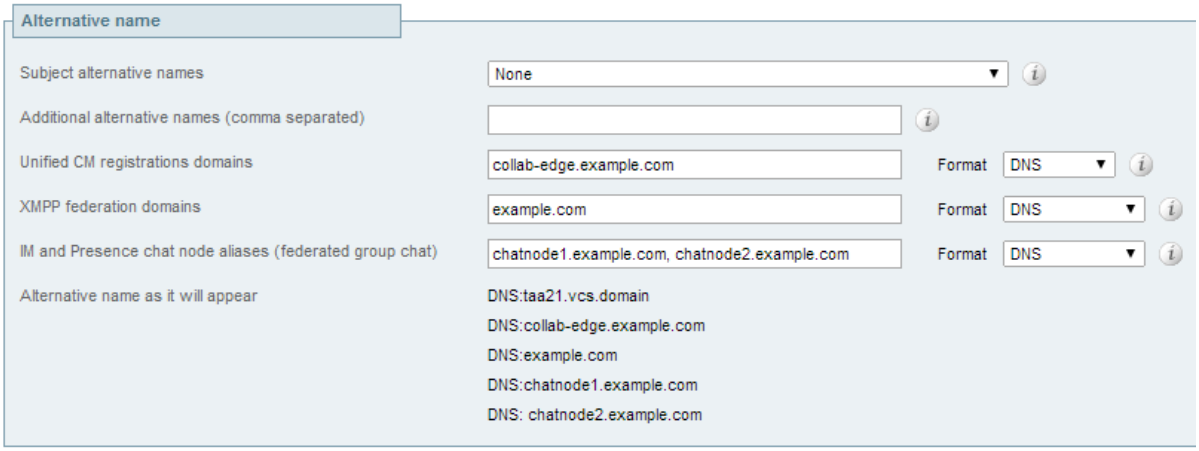


VCS Expressway server certificate requirements

The VCS Expressway server certificate needs to include the following elements in its list of subject alternate names:

- **Unified CM registrations domains**: all of the domains which are configured on the VCS Control for Unified CM registrations. They are required for secure communications between endpoint devices and VCS Expressway.
  You must select the *DNS* format and manually specify the required FQDNs, separated by commas if you need multiple domains. The *SRVName* format may not be supported by your chosen CA.
  You must also prefix each with **`collab-edge.`** (see example in following screenshot).
- **XMPP federation domains**: the domains used for point-to-point XMPP federation. These are configured on the IM&P servers and should also be configured on the VCS Control as domains for XMPP federation. We recommend that you select the *DNS* format and manually specify the required FQDNs, separated by commas if you need multiple domains. The *XMPPAddress* format may not be supported by your chosen CA.
- **IM and Presence chat node aliases (federated group chat)**: the same set of **Chat Node Aliases** as entered on the VCS Control's certificate. They are only required for voice and presence deployments which will support group chat over TLS with federated contacts.
  We recommend that you select the *DNS* format and manually specify the required FQDNs, separated by commas if you need multiple domains. The *XMPPAddress* format may not be supported by your chosen CA.
  Note that the list of required aliases can be viewed (and copy-pasted) from the equivalent **Generate CSR** page on the VCS Control.

Figure 4: Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the VCS Expressway's CSR generator



Mobile and remote access port reference

This section summarizes the ports that need to be opened on the firewalls between your internal network (where the VCS Control is located) and the DMZ (where the VCS Expressway is located) and between the DMZ and the public internet.

Outbound from VCS Control (private) to VCS Expressway (DMZ)

Purpose	Protocol	VCS Control (source)	VCS Expressway (listening)
XMPP (IM and Presence)	TCP	Ephemeral port	7400
SSH (HTTP/S tunnels)	TCP	Ephemeral port	2222
Traversal zone SIP signaling	TLS	25000 to 29999	7001
Traversal zone SIP media (for small/medium systems on X8.1 or later)	UDP	36000 to 59999*	36000 (RTP), 36001 (RTCP) (defaults) 2776 (RTP), 2777 (RTCP) (old defaults*)
Traversal zone SIP media (for large systems)	UDP	36000 to 59999*	36000 to 36011 (6 pairs of RTP and RTCP ports for multiplexed media traversal)

Outbound from VCS Expressway (DMZ) to public internet

Purpose	Protocol	VCS Expressway (source)	Internet endpoint (listening)
SIP media	UDP	36002 to 59999 or 36012 to 59999	>= 1024
SIP signaling	TLS	25000 to 29999	>= 1024

Inbound from public internet to VCS Expressway (DMZ)

Purpose	Protocol	Internet endpoint (source)	VCS Expressway (listening)
XMPP (IM and Presence)	TCP	>= 1024	5222
HTTP proxy (UDS)	TCP	>= 1024	8443
Media	UDP	>= 1024	36002 to 59999 or 36012 to 59999*
SIP signaling	TLS	>= 1024	5061
HTTPS (administrative access)	TCP	>= 1024	443

From VCS Control to Unified CM / CUC

Purpose	Protocol	VCS Control (source)	Unified CM (listening)
XMPP (IM and Presence)	TCP	Ephemeral port	7400 (IM and Presence)
HTTP proxy (UDS)	TCP	Ephemeral port	8443 (Unified CM)
HTTP proxy (SOAP)	TCP	Ephemeral port	8443 (IM and Presence Servers)
HTTP (configuration file retrieval)	TCP	Ephemeral port	6970
CUC (voicemail)	TCP	Ephemeral port	443 (CUC)
Media	UDP	36000 to 59999*	>= 1024
SIP signaling	TCP	25000 to 29999	5060
Secure SIP signaling	TLS	25000 to 29999	5061

* On new installations of X8.1 or later, the default media traversal port range is 36000 to 59999, and is set on the VCS Control (**Configuration > Local Zones > Traversal Subzone**). In Large VCS Expressway systems the first 12 ports in the range – 36000 to 36011 by default – are always reserved for multiplexed traffic. The VCS Expressway listens on these ports. You cannot configure a distinct range of demultiplex listening ports on Large systems: they always use the first 6 pairs in the media port range. On Small/Medium systems you can explicitly specify which 2 ports listen for multiplexed RTP/RTCP traffic, on the VCS Expressway (**Configuration > Traversal > Ports**). On upgrades to X8.2 or later, the VCS Control retains the media traversal port range from the previous version (could be 50000 - 54999 or 36000 - 59999, depending on source version). The VCS Expressway retains the previously configured demultiplexing pair (either 2776 & 2777 or 50000 & 50001 by default, depending on upgrade path) and the switch **Use configured demultiplexing ports** is set to *Yes*. If you do not want to use a particular pair of ports, switch **Use configured demultiplexing ports** to *No*, then the VCS Expressway will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default). In this case, we recommend that you close the previously configured ports after you configure the firewall for the new ports.

Note that:

- Ports 8191/8192 TCP and 8883/8884 TCP are used internally within the VCS Control and the VCS Expressway applications. Therefore these ports must not be allocated for any other purpose. The VCS Expressway listens externally on port 8883; therefore we recommend that you create custom firewall rules on the external LAN interface to drop TCP traffic on that port.
- The VCS Expressway listens on port 2222 for SSH tunnel traffic. The only legitimate sender of such traffic is the VCS Control (cluster). Therefore we recommend that you create the following firewall rules for the SSH tunnels service:
  - one or more rules to allow all of the VCS Control peer addresses (via the internal LAN interface, if appropriate)
  - followed by a lower priority (higher number) rule that drops all traffic for the SSH tunnels service (on the internal LAN interface if appropriate, and if so, another rule to drop all traffic on the external interface)

Additional information

Unified CM dial plan

The Unified CM dial plan is not impacted by devices registering via VCS. Remote and mobile devices still register directly to Unified CM and their dial plan will be the same as when it is registered locally.

VCS call types and licensing

The VCS distinguishes between the following types of call:

- **Unified CM remote sessions**: these are "mobile and remote access" calls i.e.video or audio calls from devices located outside the enterprise that are routed via the Expressway firewall traversal solution to endpoints registered to Unified CM. These calls do not consume any type of call license.
- **VCS traversal calls**: these are standard VCS video or audio calls, including business-to-business calls, B2BUA calls (for media encryption or ICE), and interworked or gatewayed calls to third-party solutions where the VCS takes both the call signaling and the call media. Each call consumes a traversal call license.
  Audio-only SIP traversal calls are treated distinctly from video SIP traversal calls. Each traversal call license allows either 1 video call or 2 audio-only SIP calls. Hence, a 100 traversal call license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other audio-only call (non-traversal, H.323 or interworked) will consume a standard video call license (traversal or non-traversal as appropriate).
- **VCS non-traversal calls**: these are standard VCS video or audio calls where the signaling passes through the VCS but the media goes directly between the endpoints, or between an endpoint and another system in the call route. Each call consumes a non-traversal call license. Note that Lync B2BUA calls are classified as non-traversal calls (even though the media does traverse the VCS).

Both **Unified CM remote sessions** and **VCS traversal calls** consume traversal call resources and each VCS has a maximum limit of 150 concurrent traversal calls (500 calls on Large VM servers).

Each VCS also allows up to 750 concurrent non-traversal calls.

Note that:

- VCS defines an "audio-only" SIP call as one that was negotiated with a single “m=” line in the SDP. Thus, for example, if a person makes a “telephone” call but the SIP UA includes an additional m= line in the SDP, the call will consume a video call license.
- While an "audio-only" SIP call is being established, it is treated (licensed) as a video call. It only becomes licensed as "audio-only" when the call setup has completed. This means that if your system approaches its maximum licensed limit, you may be unable to connect some "audio-only" calls if they are made simultaneously.

Deploying Unified CM and VCS in different domains

Unified CM nodes and VCS peers can be located in different domains. For example, your Unified CM nodes may be in the **`enterprise.com`** domain and your VCS system may be in the **`edge.com`** domain.

In this case, Unified CM nodes must use IP addresses for the **Server host name / IP address** to ensure that VCS can route traffic to the relevant Unified CM nodes.

Unified CM servers and IM&P servers must share the same domain.

SIP trunks between Unified CM and VCS Control

VCS deployments for mobile and remote access do not require SIP trunk connections between Unified CM and VCS Control. Note that the automatically generated neighbor zones between VCS Control and each discovered Unified CM node are not SIP trunks.

However, you may still configure a SIP trunk if required (for example, to enable B2B callers or endpoints registered to VCS to call endpoints registered to Unified CM).

If a SIP trunk is configured, you must ensure that it uses a different listening port on Unified CM from that used for SIP line registrations to Unified CM. An alarm is raised on VCS Control if a conflict is detected.

Configuring line registration listening ports on Unified CM

The listening ports used for line registrations to Unified CM are configured via **System > Cisco Unified CM**.

The **SIP Phone Port** and **SIP Phone Secure Port** fields define the ports used for TCP and TLS connections respectively and are typically set to 5060/5061.

Configuring SIP trunk listening ports

The ports used for SIP trunks are configured on both Unified CM and VCS.

On Unified CM:

1. Go to **System > Security > SIP Trunk Security Profile** and select the profile used for the SIP trunk. If this profile is used for connections from other devices, you may want to create a separate security profile for the SIP trunk connection to VCS.
2. Configure the **Incoming Port** to be different from that used for line registrations.
3. Click **Save** and then click **Apply Config**.

On VCS:

1. Go to **Configuration > Zones > Zones** and select the Unified CM neighbor zone used for the SIP trunk. (Note that the automatically generated neighbor zones between VCS Control and each discovered Unified CM node for line side communications are non-configurable.)
2. Configure the SIP **Port** to the same value as the **Incoming Port** configured on Unified CM.
3. Click **Save**.

See *Cisco TelePresence Cisco Unified Communications Manager with VCS (SIP Trunk) Deployment Guide* for more information about configuring a SIP trunk.

Configuring secure communications

This deployment requires secure communications between the VCS Control and the VCS Expressway, and between the VCS Expressway and endpoints located outside the enterprise. This involves the mandating of encrypted TLS communications for HTTP, SIP and XMPP, and, where applicable, the exchange and checking of certificates. Jabber endpoints must supply a valid username and password combination, which will be validated against credentials held in Unified CM. All media is secured over SRTP.

VCS Control automatically generates non-configurable neighbor zones between itself and each discovered Unified CM node. A TCP zone is always created, and a TLS zone is created also if the Unified CM node is configured with a **Cluster Security Mode** (**System > Enterprise Parameters > Security Parameters**) of *1*

(Mixed) (so that it can support devices provisioned with secure profiles). The TLS zone is configured with its **TLS verify mode** set to *On* if the Unified CM discovery had **TLS verify mode** enabled. This means that the VCS Control will verify the CallManager certificate for subsequent SIP communications. Note that secure profiles are downgraded to use TCP if Unified CM is not in mixed mode.

The VCS neighbor zones to Unified CM use the names of the Unified CM nodes that were returned by Unified CM when the Unified CM publishers were added (or refreshed) to the VCS. The VCS uses those returned names to connect to the Unified CM node. If that name is just the host name then:

- it needs to be routable using that name
- this is the name that the VCS expects to see in the Unified CM's server certificate

If you are using secure profiles, ensure that the root CA of the authority that signed the VCS Control certificate is installed as a *CallManager-trust* certificate (**Security > Certificate Management** in the **Cisco Unified OS Administration** application).

VCS automated intrusion protection

You may need to enable the **Automated protection service** (**System > System administration**) if it is not yet running.

To protect against malicious attempts to access the HTTP proxy, you can configure automated intrusion protection on the VCS Expressway (**System > Protection > Automated detection > Configuration**).

We recommend that you enable the following categories:

- **HTTP proxy authorization failure** and **HTTP proxy protocol violation**. Note: Do not enable the **HTTP proxy resource access failure** category.
- **XMPP protocol violation**

Note: The **Automated protection service** uses Fail2ban software. It protects against brute force attacks that originate from a single source IP address.

Unified CM denial of service threshold

High volumes of mobile and remote access calls may trigger denial of service thresholds on Unified CM. This is because all the calls arriving at Unified CM are from the same VCS Control (cluster).

If necessary, we recommend that you increase the level of the **SIP Station TCP Port Throttle Threshold** (**System > Service Parameters**, and select the *Cisco CallManager* service) to 750 KB/second.

Limitations

- The IPV4 protocol only is supported for mobile and remote access users
- SIP Early Media is not supported
- In VCS Expressway systems that use dual network interfaces, XCP connections (for IM&P XMPP traffic) always use the non-external (i.e. internal) interface. This means that XCP connections may fail in deployments where the VCS Expressway internal interface is on a separate network segment and is used for system management purposes only, and where the traversal zone on the VCS Control connects to the VCS Expressway's external interface.

Unsupported Jabber features when using mobile and remote access

- Directory access mechanisms other than UDS
- Certificate provisioning to remote endpoints e.g. CAPF
- File transfer (except when operating in hybrid Webex mode)
- Deskphone control (QBE/CTI)
- Additional mobility features including DVO-R, GSM handoff and session persistency
- Self-care portal
- Support for Jabber SDK
- Shared lines are supported in a limited way. Multiple endpoints can share a line but in-call features (like hold/resume) only work on the first endpoint that answers. Endpoints sharing the line may not correctly recognise the state of the call.

Unsupported features and limitations when using mobile and remote access

- Secure XMPP traffic between VCS Control and IM&P servers (XMPP traffic is secure between VCS Control and VCS Expressway, and between VCS Expressway and remote endpoint)
- Endpoint management capability (SNMP, SSH/HTTP access)
- Multi-domain and multi-customer support; each VCS deployment supports only one IM&P domain (even though IM & Presence 10.0 or later supports multiple IM&P domains)
- Mobile and remote access functionality is not within the FIPS boundary
- The VCS Control used for Mobile and Remote Access cannot also be used as a Lync 2013 gateway (if required, this must be configured on a stand-alone VCS Control
- NTLM authentication via the HTTP proxy
- Maintenance mode; if a VCS-C or VCS Expressway is placed into maintenance mode, any existing calls passing through that VCS will be dropped
- The VCS Expressway must not have TURN services enabled
- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM (the same limit as VCS appliances or equivalent VM)

Protocol summary

The table below lists the protocols and associated services used in the Unified Communications solution.

Protocol	Security	Service
SIP	TLS	Session establishment – Register, Invite etc.
HTTPS	TLS	Logon, provisioning/configuration, directory, visual voicemail
RTP	SRTP	Media - audio, video, content sharing
XMPP	TLS	Instant Messaging, Presence

Clustered VCS systems and failover considerations

You can configure a cluster of VCS Controls and a cluster of VCS Expressways to provide failover (redundancy) support as well as improved scalability.

Details about how to set up VCS clusters are contained in *VCS Cluster Creation and Maintenance Deployment Guide* and information about how to configure Jabber endpoints and DNS are contained in *Configure DNS for Cisco Jabber*.

Note that when discovering Unified CM and IM&P servers on VCS Control, you must do this on the master peer.

Media encryption

Media encryption is enforced on the call legs between the VCS Control and the VCS Expressway, and between the VCS Expressway and endpoints located outside the enterprise. Call legs between VCS Control and endpoints within the enterprise will not be encrypted.

The encryption is physically applied to the media as it passes through the B2BUA on the VCS Control.

Advanced VCS Control configuration

This section covers the advanced Unified Communications settings that can be configured on VCS Control.

Credential caching intervals

The VCS caches endpoint credentials which have been authenticated by Unified CM. The caching of credentials reduces the frequency with which the VCS has to submit endpoint credentials to Unified CM for authentication, and thus improves system performance.

To configure the caching settings, go to **Configuration > Unified Communications** and then click **Show advanced settings**.

The **Credentials refresh interval** specifies the number of minutes for which endpoint credentials are cached in the VCS database. The default is 480 minutes.

The **Credentials cleanup interval** specifies the frequency with which the VCS database runs a cleanup process to remove expired credentials. In large deployments, a regular cleanup process helps to maintain the system's performance. The default is 720 minutes.

Appendix 1: Troubleshooting

General troubleshooting techniques

Checking alarms and status

When troubleshooting any issue, we recommend that you first check if any alarms have been raised (**Status > Alarms**). If alarms exist, follow the instructions provided in the **Action** column. You should check the alarms on both VCS Control and VCS Expressway.

Next, go to **Status > Unified Communications** to see a range of status summary and configuration information. You should check this status page on both VCS Control and VCS Expressway.

If any required configuration is missing or invalid an error message is shown and a link to the relevant configuration page is provided.

You may see invalid services or errors if you have changed any of the following items on VCS:

- server or CA certificates
- DNS configuration
- domain configuration

In these cases, a system restart is required to ensure that those configuration changes take effect.

Checking and taking diagnostic logs

Jabber for Windows

The Jabber for Windows log file is saved as **csf-unified.log** under **C:\Users\<UserID>\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs**.

The configuration files are located under **C:\Users\<UserID>\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Config**.

Performing VCS diagnostic logging

The diagnostic logging tool in VCS can be used to assist in troubleshooting system issues. It allows you to generate a diagnostic log of system activity over a period of time, and then to download the log.

Before taking a diagnostic log, you must configure the log level of the relevant logging modules:

1. Go to **Maintenance > Diagnostics > Advanced > Support Log configuration**.
2. Select the following logs:
   - developer.edgeconfigprovisioning
   - developer.trafficserver
   - developer.xcp
3. Click **Set to debug**.

You can now start the diagnostic log capture:

1. Go to **Maintenance > Diagnostics > Diagnostic logging**.
2. Optionally, select **Take tcpdump while logging**.
3. Click **Start new log**.

4. (Optional) Enter some **Marker** text and click **Add marker**.
   - The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
   - You can add as many markers as required, at any time while the diagnostic logging is in progress.
   - Marker text is added to the log with a "**DEBUG_MARKER**" tag.
5. Reproduce the system issue you want to trace in the diagnostic log.
6. Click **Stop logging**.
7. Click **Download log** to save the diagnostic log archive to your local file system. You are prompted to save the archive (the exact wording depends on your browser).

After you have completed your diagnostic logging, return to the **Support Log configuration** page and reset the modified logging modules back to *INFO* level.

Checking DNS records

You can use the VCS's DNS lookup tool (**Maintenance > Tools > Network utilities > DNS lookup**) to assist in troubleshooting system issues. The SRV record lookup includes those specific to H.323, SIP, Unified Communications and TURN services.

Note that performing the DNS lookup from the VCS Control will return the view from within the enterprise, and that performing it on the VCS Expressway will return what is visible from within the DMZ which is not necessarily the same set of records available to endpoints in the public internet.

The DNS lookup includes the following SRV services that are used for Unified Communications:

- _collab-edge._tls
- _collab-edge._tcp
- _cuplogin._tcp
- _cisco-uds._tcp

Checking reachability of the VCS Expressway

Ensure that the FQDN of the VCS Expressway is resolvable in public DNS.

The FQDN is configured at **System > DNS** and is built as <**System host name**>.<**Domain name**>.

Checking call status

Call status information can be displayed for both current and completed calls:

- **Current calls**: the **Call status** page (**Status > Calls > Calls**) lists all the calls currently taking place to or from devices registered with the VCS, or that are passing through the VCS.
- **Completed calls**: the **Call history** page (**Status > Calls > History**) lists all the calls that are no longer active. The list is limited to the most recent 500 calls, and only includes calls that have taken place since the VCS was last restarted.

The same set of call status information is also shown on the **Calls by registration** page (accessed via the **Registration details** page).

If the VCS is part of a cluster, all calls that apply to any peer in the cluster are shown, although the list is limited to the most recent 500 calls per peer.

Identifying mobile and remote access calls

The call status and call history pages show all call types: Unified CM remote sessions (if mobile and remote access is enabled) as well as VCS traversal and non-traversal calls.

To distinguish between the call types you must drill down into the call components. Mobile and remote access calls have different component characteristics depending on whether the call is being viewed on the VCS Control or VCS Expressway:

- On a VCS-C, a Unified CM remote session will have 3 components (as it uses the B2BUA to enforce media encryption). One of the VCS components will route the call through one of the automatically generated neighbor zones (with a name prefixed by either **CEtcp** or **CEtls**) between VCS and Unified CM.
- On a VCS-E, there will be one component and that will route the call through the **CollaborationEdgeZone**.

Note that if both endpoints are outside of the enterprise (i.e. off premises), you will see this treated as 2 separate calls.

Checking devices registered to Unified CM via VCS

Identifying devices in Unified CM

To identify devices registered to Unified CM via VCS:

1. In Unified CM, go to **Device > Phone** and click **Find**.
2. Check the **IP Address** column. Devices that are registered via VCS will display an **IP Address** of the VCS Control it is registered through.

Identifying provisioned sessions in VCS Control

To identify sessions that have been provisioned via VCS Control:

1. In VCS Control, go to **Status > Unified Communications**.
2. In the **Advanced status information** section, click **View provisioning sessions**.
   This shows a list of all current and recent (shown in red) provisioning sessions.

Ensuring that VCS Control is synchronized to Unified CM

Changes to Unified CM cluster or node configuration can lead to communication problems between Unified CM and VCS Control. This includes changes to:

- the number of nodes within a Unified CM cluster
- the host name or IP address of an existing node
- listening port numbers
- security parameters
- phone security profiles

You must ensure that any such changes are reflected in the VCS Control. To do this you must rediscover all Unified CM and IM & Presence nodes (on VCS go to **Configuration > Unified Communications**).

VCS certificate / TLS connectivity issues

If the VCS's server certificate or trusted CA certificates have been modified, you must restart the VCS before those changes will take effect.

If you are using secure profiles, ensure that the root CA of the authority that signed the VCS Control certificate is installed as a *CallManager-trust* certificate (**Security > Certificate Management** in the **Cisco Unified OS Administration** application).

VCS returns "401 unauthorized" failure messages

A "401 unauthorized" failure message can occur when the VCS attempts to authenticate the credentials presented by the endpoint client.The reasons for this include:

- The client is supplying an unknown username or the wrong password.
- ILS (Intercluster Lookup Service) has not been set up on all of the Unified CM clusters. This may result in intermittent failures, depending upon which Unified CM node is being used by VCS for its UDS query to discover the client's home cluster.

Call failures due to "407 proxy authentication required" or "500 Internal Server Error" errors

Call failures can occur if the traversal zones on VCS are configured with an **Authentication policy** of *Check credentials*. Ensure that the **Authentication policy** on the traversal zones used for mobile and remote access is set to *Do not check credentials*.

Call bit rate is restricted to 384 kbps / video issues when using BFCP (presentation sharing)

This can be caused by video bit rate restrictions within the regions configured on Unified CM.

Ensure that the **Maximum Session Bit Rate for Video Calls** between and within regions (**System > Region Information > Region**) is set to a suitable upper limit for your system, for example 6000 kbps.

Endpoints cannot register to Unified CM

Endpoints may fail to register for various reasons:

- Endpoints may not be able to register to Unified CM if there is also a SIP trunk configured between Unified CM and VCS Control. If a SIP trunk is configured, you must ensure that it uses a different listening port on Unified CM from that used for SIP line registrations to Unified CM. See SIP trunks between Unified CM and VCS Control [p.30] for more information.
- Secure registrations may fail ('Failed to establish SSL connection' messages) if the server certificate on the VCS Control does not contain in its Subject Alternate Name list, the names of all of the Phone Security Profiles in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Note that these names — in both Unified CM and in the VCS's certificate — must be in FQDN format.

Jabber cannot sign in due to XMPP bind failure

The Jabber client may be unable to sign in ("Cannot communicate with the server" error messages) due to XMPP bind failures.

This will be indicated by resource bind errors in the Jabber client logs, for example:

```
XmppSDK.dll #0, 201, Recv:<iq id='uid:527a7fe7:00000cfe:00000000' type='error'><bind
xmlns='urn:ietf:params:xml:ns:xmpp-bind'/><error code='409' type='cancel'><conflict
xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/></error></iq>
XmppSDK.dll #0, CXmppClient::onResourceBindError
XmppSDK.dll #0, 39, CTriClient::HandleDisconnect, reason:16
```

This typically occurs if the IM and Presence Intercluster Sync Agent is not working correctly. See IM and Presence intercluster deployment configuration for more information.

No voicemail service ("403 Forbidden" response)

Ensure that the Cisco Unity Connection (CUC) hostname is included on the HTTP server allow list on the VCS Control.

"403 Forbidden" responses for any service requests

Services may fail ("403 Forbidden" responses) if the VCS Control and VCS Expressway are not synchronized to a reliable NTP server. Ensure that all VCS systems are synchronized to a reliable NTP service.

Client HTTPS requests are dropped by VCS

This can be caused by the automated intrusion protection feature on the VCS Expressway if it detects repeated invalid attempts (404 errors) from a client IP address to access resources through the HTTP proxy.

To prevent the client address from being blocked, ensure that the **HTTP proxy resource access failure** category (**System > Protection > Automated detection > Configuration**) is disabled.

Unable to configure IM&P servers for remote access

'Failed: <address> is not a IM and Presence Server'

This error can occur when trying to configure the IM&P servers used for remote access (via **Configuration > Unified Communications > IM and Presence servers**).

It is due to missing CA certificates on the IM&P servers and applies to systems running 9.1.1. More information and the recommended solution is described in bug CSCul05131.

Jabber cannot sign in due to SSH tunnels failure

Jabber can fail to sign in due to the SSH tunnels failing to be established. The traversal zone between the VCS Control and VCS Expressway will work normally in all other respects. VCS will report 'Application failed - An unexpected software error was detected in portforwarding.pyc'.

This can occur if the VCS Expressway DNS hostname contains underscore characters. You must ensure the hostname only contain letters, digits and hyphens.

Document revision history

The following table summarizes the changes that have been applied to this document.

Date	Description
January 2015	Re-issued X8.2 version with section on discovering Cisco Unity Connection servers removed.
January 2015	Re-issued X8.2 version with updated firewall advice in configuration summary.
November 2014	Re-issued X8.2 version to clarify media port ranges.
August 2014	Re-issued X8.1.1 version of this document with shared line limitation, as per X8.2 version.
July 2014	Re-issued with updated client support details and a media encryption limitation removed.
July 2014	Re-issued with updated firewall advice and unsupported deployment.
July 2014	Re-issued with updated domains screenshot.
June 2014	Republished for X8.2.
April 2014	Initial release.