Cisco TelePresence Device Authentication on Cisco VCS

Deployment Guide

Cisco VCS X8.2

D14819.08

June 2014

Contents

About device authentication

Device authentication is the verification of the credentials of an incoming request to the VCS from a device or external system. It is used so that certain functionality may be reserved for known and trusted users, for example the publishing of presence status, collection of provisioning data, or the ability to use resources that cost money like ISDN gateway calling.

When device authentication is enabled on a VCS, any device that attempts to communicate with the VCS is challenged to present its credentials (typically based on a username and password). The VCS will then verify those credentials, or have them verified, according to the authentication method, and then accept or reject the message accordingly.

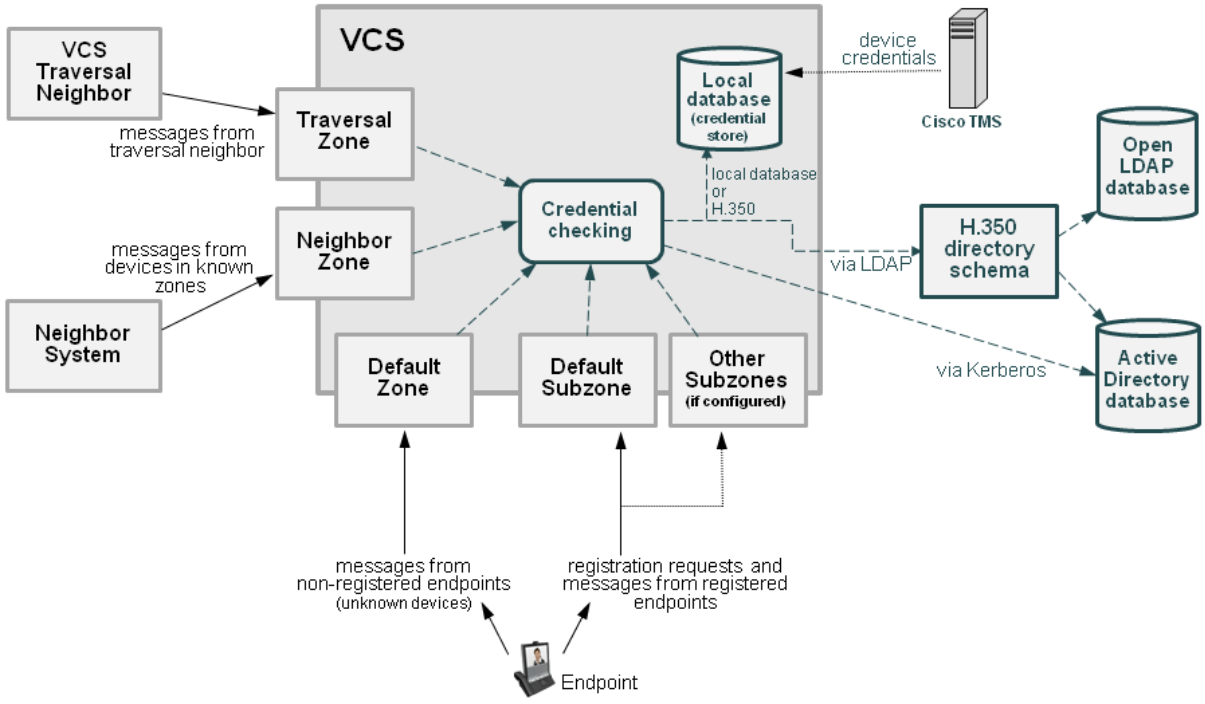
VCS authentication policy can be configured separately for each zone and subzone. This means that both authenticated and unauthenticated devices could be allowed to register to, and communicate with, the same VCS if required. Subsequent call routing decisions can then be configured with different rules based upon whether a device is authenticated or not.

The VCS attempts to verify the credentials presented to it by first checking against its on-box local database of usernames and passwords. The local database also includes checking against credentials supplied by Cisco TMS if your system is using device provisioning. If the username is not found in the local database, the VCS may then attempt to verify the credentials via a real-time LDAP connection to an external H.350 directory service. The directory service, if configured, must have an H.350 directory schema for either a Microsoft Active Directory LDAP server or an OpenLDAP server.

You can also configure a VCS-E so that the credential checking of SIP messages is delegated, via a traversal zone, to another VCS.

Along with one of the above methods, for those devices that support NTLM challenges, the VCS can alternatively verify credentials via direct access to an Active Directory server using a Kerberos connection.

The various VCS authentication entry points and credential checking methods are shown below:



Unified Communications mobile and remote access devices

You do not have to make any explicit configuration on the VCS regarding the authentication of devices that are registering to Unified CM via the VCS. The VCS automatically handles the authentication of these devices against its home Unified CM cluster.

Authentication policy

Configuring VCS authentication policy

Authentication policy is applied by the VCS at the zone and subzone levels. It controls how the VCS challenges incoming messages (for provisioning, registration, presence, phone books and calls) from that zone or subzone and whether those messages are rejected, treated as authenticated, or treated as unauthenticated within the VCS.

Each zone and subzone can set its **Authentication policy** to either *Check credentials*, *Do not check credentials*, or *Treat as authenticated*.

- Registration authentication is controlled by the Default Subzone (or relevant alternative subzone) configuration.
- Initial provisioning subscription request authentication is controlled by the Default Zone configuration.
- Call, presence, and phone book request authentication is controlled by the Default Subzone (or relevant alternative subzone) if the endpoint is registered, or by the Default Zone if the endpoint is not registered.

Note that the exact authentication policy behavior depends on whether the messages are H.323 messages, SIP messages received from local domains, or SIP messages received from non-local domains. See Authentication policy configuration options [p.8] for a full description of the various authentication policy behaviors.

Zone-level authentication policy

Authentication policy is configurable for zones that receive messaging; the Default Zone, neighbor zones, traversal client and traversal server zones all allow configuration of authentication policy; DNS and ENUM zones do not receive messaging and so have no configuration.

To configure a zone's **Authentication policy**, go to **Configuration > Zones > Zones**, then click View/Edit or the name of the zone. The policy is set to *Do not check credentials* by default when a new zone is created.

Subzone-level authentication policy

Authentication policy is configurable for the Default Subzone and any other configured subzone.

To configure a subzone's **Authentication policy**, go to **Configuration > Local Zone > Subzones**, then click View/Edit or the name of the subzone. The policy is set to *Do not check credentials* by default when a new subzone is created.

Provisioning and device authentication

The Provisioning Server requires that any provisioning or phone book requests it receives have already been authenticated at the zone or subzone point of entry into the VCS. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

See Device provisioning and authentication policy [p.15] for more information.

Presence and device authentication

The Presence Server accepts presence PUBLISH messages only if they have already been authenticated:

- The authentication of presence messages by the VCS is controlled by the authentication policy setting on the Default Subzone (or relevant alternative subzone) if the endpoint is registered (which is the usual case), or by the authentication policy setting on the Default Zone if the endpoint is not registered.

- The relevant **Authentication policy** must be set to either *Check credentials* or *Treat as authenticated*, otherwise PUBLISH messages will fail, meaning that endpoints will not be able to publish their presence status.

See Presence and authentication policy [p.17] for more information.

Controlling system behavior for authenticated and non-authenticated devices

How calls and other messaging from authenticated and non-authenticated devices are handled depends on how search rules, external policy services and CPL are configured.

Search rules

When configuring a search rule, use the **Request must be authenticated** attribute to specify whether the search rule applies only to authenticated search requests or to all requests.

External policy services

External policy services are typically used in deployments where policy decisions are managed through an external, centralized service rather than by configuring policy rules on the VCS itself. You can configure the VCS to use policy services in the following areas:

- Registration Policy
- Search rules (dial plan)
- Call Policy
- User Policy (FindMe)

When the VCS uses a policy service it sends information about the call or registration request to the service in a POST message using a set of name-value pair parameters. Those parameters include information about whether the request has come from an authenticated source or not.

More information about policy services, including example CPL, can be found in *External Policy on VCS Deployment Guide*.

CPL

If you are using the Call Policy rules generator on the VCS, source matches are carried out against authenticated sources. To specify a match against an unauthenticated source, just use a blank field. (If a source is not authenticated, its value cannot be trusted).

If you use uploaded, handcrafted local CPL to manage your Call Policy, you are recommended to make your CPL explicit as to whether it is looking at the authenticated or unauthenticated origin.

- If CPL is required to look at the unauthenticated origin (for example, when checking non-authenticated callers) the CPL must use `unauthenticated-origin`. (However, if the user is unauthenticated, they can call themselves whatever they like; this field does not verify the caller.)
- To check the authenticated origin (only available for authenticated or “treat as authenticated” devices) the CPL should use `authenticated-origin`.

Note that due to the complexity of writing CPL scripts, you are recommended to use an external policy service instead.

Authentication policy configuration options

Authentication policy behavior varies for H.323 messages, SIP messages received from local domains and SIP messages from non-local domains.

The primary authentication policy configuration options and their associated behavior are as follows:

- **Check credentials**: verify the credentials using the relevant authentication method. Note that in some scenarios, messages are not challenged, see below.
- **Do not check credentials**: do not verify the credentials and allow the message to be processed.
- **Treat as authenticated**: do not verify the credentials and allow the message to be processed as if it is has been authenticated. This option can be used to cater for endpoints from third-party suppliers that do not support authentication within their registration mechanism. Note that in some scenarios, messages are allowed but will still be treated as though they are unauthenticated, see below.

The following tables summarize the policy behavior when applied at the zone and subzone level, and how it varies depending on the message protocol.

Zone-level authentication policy

Authentication policy is configurable for zones that receive messaging; the Default Zone, neighbor zones, traversal client and traversal server zones all allow configuration of authentication policy; DNS and ENUM zones do not receive messaging and so have no configuration.

To configure a zone's **Authentication policy**, go to **Configuration > Zones > Zones**, then click View/Edit or the name of the zone. The policy is set to *Do not check credentials* by default when a new zone is created.

The behavior varies for H.323 and SIP messages as shown in the tables below:

H.323

Policy	Behavior
Check credentials	Messages are classified as either authenticated or unauthenticated depending on whether any credentials in the message can be verified against the authentication database. If no credentials are supplied, the message is always classified as unauthenticated.
Do not check credentials	Message credentials are not checked and all messages are classified as unauthenticated.
Treat as authenticated	Message credentials are not checked and all messages are classified as authenticated.

SIP

The behavior for SIP messages at the zone level depends upon the **SIP authentication trust mode** setting (meaning whether the VCS trusts any pre-existing authenticated indicators - known as P-Asserted-Identity headers - within the received message) and whether the message was received from a local domain (a domain for which the VCS is authoritative) or a non-local domain.

Policy	Trust	In local domain	Outside local domain
Check credentials	Off	Messages are challenged for authentication. Messages that fail authentication are rejected. Messages that pass authentication are classified as authenticated and a P-Asserted-Identity header is inserted into the message.	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.
	On	Messages with an existing P-Asserted-Identity header are classified as authenticated, without further challenge. The P-Asserted-Identity header is passed on unchanged (keeping the originator's asserted ID). Messages without an existing P-Asserted-Identity header are challenged. If authentication passes, the message is classified as authenticated and a P-Asserted-Identity header is inserted into the message. If authentication fails, the message is rejected.	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.
Do not check credentials	Off	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.
	On	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.
Treat as authenticated	Off	Messages are not challenged for authentication. All messages are classified as authenticated. Any existing P-Asserted-Identity header is removed and a new one containing the VCS's originator ID is inserted into the message.	Messages are not challenged for authentication. All messages are classified as unauthenticated. Any existing P-Asserted-Identity headers are removed.

Policy	Trust	In local domain	Outside local domain
	On	Messages are not challenged for authentication. All messages are classified as authenticated. Messages with an existing P-Asserted-Identity header are passed on unchanged. Messages without an existing P-Asserted-Identity header have one inserted.	Messages are not challenged for authentication. Messages with an existing P-Asserted-Identity header are classified as authenticated, and the header is passed on unchanged. Messages without an existing P-Asserted-Identity header are classified as unauthenticated.

Subzone-level authentication policy

Authentication policy is configurable for the Default Subzone and any other configured subzone.

To configure a subzone's **Authentication policy**, go to **Configuration > Local Zone > Subzones**, then click View/Edit or the name of the subzone. The policy is set to *Do not check credentials* by default when a new subzone is created.

The behavior varies for H.323 and SIP messages as shown in the tables below:

H.323

Policy	Behavior
Check credentials	Messages are classified as either authenticated or unauthenticated depending on whether any credentials in the message can be verified against the authentication database. Messages that pass authentication are classified as authenticated. If no credentials are supplied, the message is always classified as unauthenticated. Note that unauthenticated registration requests are rejected.
Do not check credentials	Message credentials are not checked and all messages are classified as unauthenticated.
Treat as authenticated	Message credentials are not checked and all messages are classified as authenticated.

SIP

The behavior for SIP messages depends upon whether the message was received from a local domain (a domain for which the VCS is authoritative) or a non-local domain.

Policy	In local domain	Outside local domain
Check credentials	Messages are challenged for authentication and those that pass are classified as authenticated. Messages (including registration requests) that fail authentication are rejected.	SIP messages received from non-local domains are all treated in the same manner, regardless of the subzone's **Authentication policy** setting: Messages are not challenged for authentication. All messages are classified as unauthenticated.
Do not check credentials	Messages are not challenged for authentication. All messages are classified as unauthenticated.	
Treat as authenticated	Messages are not challenged for authentication. All messages are classified as authenticated.	

SIP authentication trust

If the VCS is configured to use device authentication it will authenticate incoming SIP registration and INVITE requests. If the VCS then forwards the request on to a neighbor zone such as another VCS, that receiving system will also authenticate the request. In this scenario the message has to be authenticated at every hop.

To simplify this so that a device's credentials only have to be authenticated once (at the first hop), and to reduce the number of SIP messages in your network, you can configure neighbor zones to use the **Authentication trust mode** setting.

This is then used in conjunction with the zone's authentication policy to control whether pre-authenticated SIP messages received from that zone are trusted and are subsequently treated as authenticated or unauthenticated within the VCS. Pre-authenticated SIP requests are identified by the presence of a P-Asserted-Identity field in the SIP message header as defined by *RFC 3325*.

The **Authentication trust mode** settings are:

- *On*: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the VCS. Unauthenticated messages are challenged if the **Authentication policy** is set to *Check credentials*.
- *Off*: any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the **Authentication policy** is set to *Check credentials*.

Note:

- We recommend that you enable authentication trust only if the neighbor zone is part of a network of trusted SIP servers.
- Authentication trust is automatically implied between traversal server and traversal client zones.

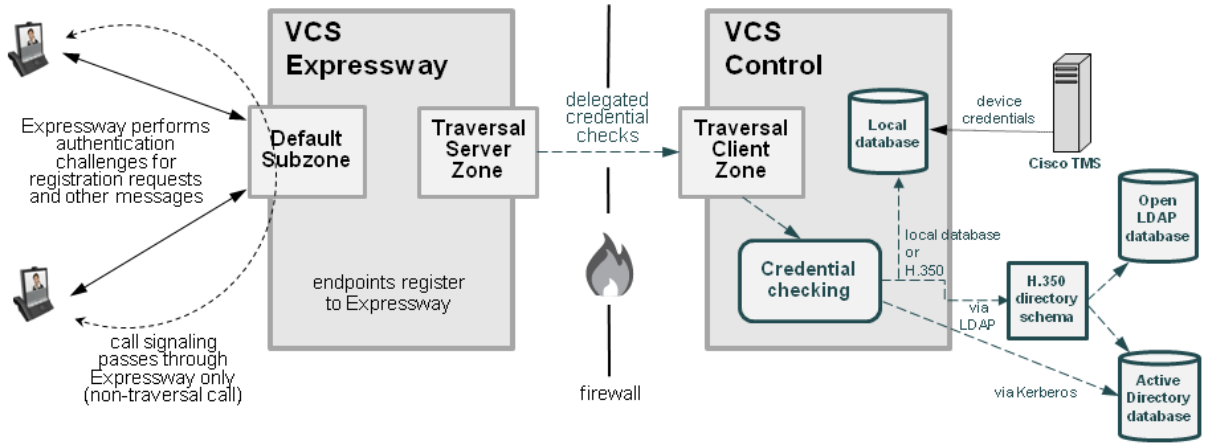
Configuring delegated credential checking (SIP only)

By default, the VCS uses the relevant credential checking mechanisms (local database, Active Directory Service or H.350 directory via LDAP) on the same VCS that is performing the authentication challenge.

Alternatively you can configure the VCS that is performing the authentication challenges to delegate the credential checking of SIP messages, via a traversal zone, to another VCS (typically a VCS-C). Delegated credential checking is useful in deployments where you want to allow devices to register on the VCS Expressway (so that, for example, calls may be made without having to use a traversal license), but for security you want all communications with authentication systems (such as an Active Directory server) to be performed inside the enterprise.

- Credential checking for both SIP Digest and NTLM messages may be delegated.
- All messages must be for locally-defined SIP domains. You can delegate credential checking to different traversal clients on a per domain basis if required.

The following diagram shows how incoming SIP messages (calls, registrations and so on) are challenged by the VCS Expressway, but the checking of the credentials presented in response to those challenges is delegated to the VCS Control.



Configuring your video communications network for delegated credential checking

Several configuration steps are involved, on both your VCS Expressway and your VCS Control, in setting up your video network for delegated credential checking.

It is likely that much of this configuration, such as the set of local SIP domains, will already be in place, however the sections below list all of the necessary configuration requirements.

VCS Expressway and VCS Control

There must be 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.

VCS Control

1. Configure SIP domains (**Configuration > Domains**).
   It must be configured with all of the domains for which it will receive delegated authentication checks.
2. Configure the relevant authentication mechanisms (local database, Active Directory Service or H.350 directory via LDAP).
3. Enable **Delegated credential checking** (**Configuration > Protocols > SIP**).
4. Ensure that the traversal client zone is configured to **Accept delegated credential checks**.

VCS Expressway

1. Configure SIP domains (**Configuration > Domains**).
   It must be configured with all of the domains for which it will delegate authentication checks.
2. For each domain, choose the traversal zone over which the credential checks are to be delegated.
3. If NTLM / Active Directory Service authentication is required, ensure that **NTLM protocol challenges** (**Configuration > Authentication > Devices > Active Directory Service**) is set to *Auto*.
4. Enable **Delegated credential checking** on the **SIP** page (**Configuration > Protocols > SIP**).
5. Ensure that the relevant zone and subzone authentication policies are set to *Check credentials*.
   Note that any H.323 messages that arrive at the zones or subzones that are now configured to *Check credentials* will still have those credentials checked via the relevant mechanisms (such as the local database or H.350 directory) on that local VCS and they will not be delegated.
6. If required as part of your dial plan, configure search rules that forward SIP call signaling messages to the relevant traversal client zones.
   (Note that no specific search rules are required to support the delegation of authentication messages to the VCS Control.

The credential checking of authentication challenges made by the VCS Expressway should now be delegated through the traversal zone to the VCS Control.

Testing the credential checking service

To verify whether the VCS to which credential checking has been delegated is able to receive messages and perform the relevant authentication checks:

1. Go to **Configuration > Domains**.
2. Select the relevant domains.
3. Click **Test credential checking service**.
   The system displays a **Results** section and reports whether the receiving VCS can be reached over the traversal zone and, additionally, if it is able to perform credential checking for both NTLM and SIP digest type challenges.
   If you are not using NTLM authentication in your video network, and thus the receiving VCS is not configured with a connection to an Active Directory Service, then the NTLM check will be expected to fail.

TURN services

If TURN services are enabled on the VCS Expressway and you also want to delegate the credential checking of TURN server requests:

1. Go to **Configuration > Traversal > TURN**.
2. Set **Delegated credential checking** to *On*.
3. For the **Authentication realm**, choose from the set of configured SIP domains to determine the traversal zone through which credential checking is delegated.

Additional information

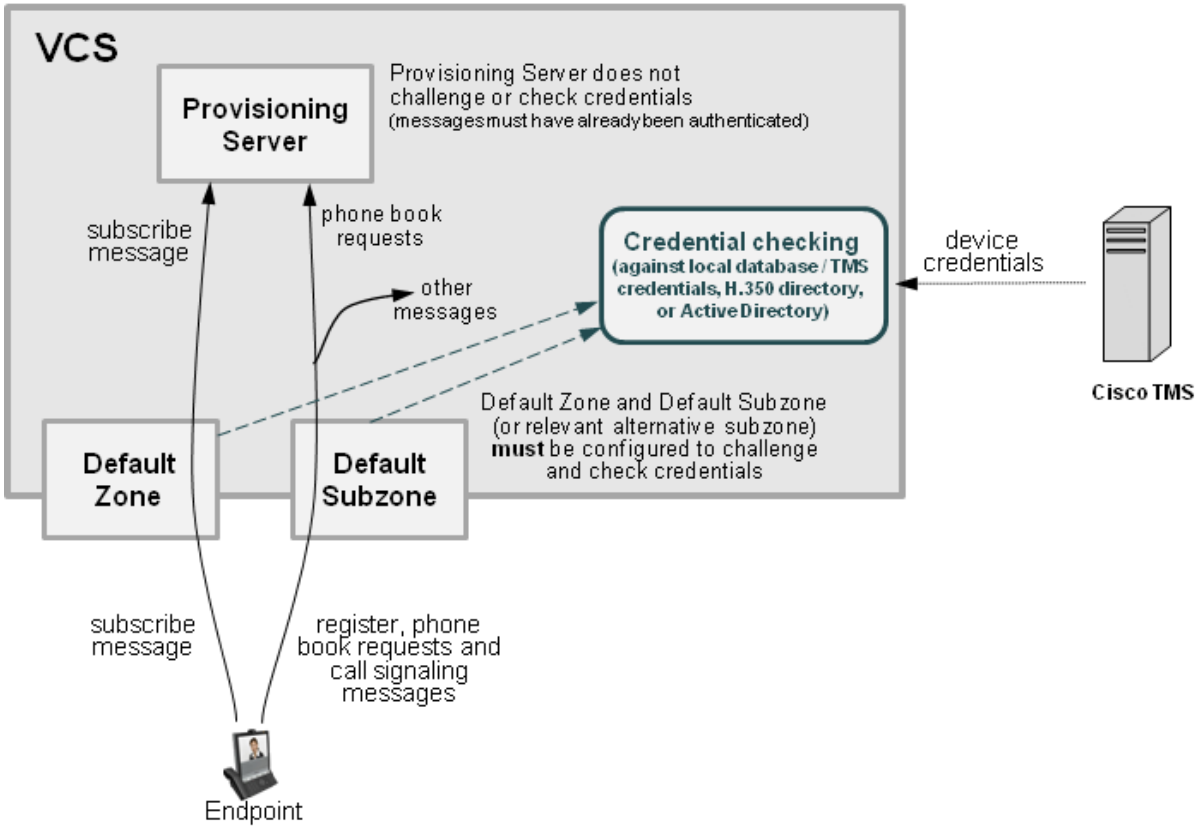
- The system clocks on the VCS Control and the VCS Expressway must be within 100 seconds of each other. We recommend that all VCSs are configured to use a common NTP server.
- The VCS Expressway can still perform "local" non-delegated authentication for specific domains. If this is required, ensure that:
  - Those domains have **Traversal zone for delegated credential checking** set to *Do not delegate*.
  - The relevant authentication mechanisms are configured on the VCS Expressway.
- The VCS Control can still perform authentication in the normal manner, as well as providing a delegated credential checking service for the VCS Expressway. Note that:
  - The **NTLM protocol challenges** setting on the VCS Control only applies if the VCS Control itself is making an authentication challenge.
  - The authentication policy configuration on the traversal client on the VCS Control has no effect on the delegated credential checking requests received by the VCS Control.

  Enabling delegated credential checking does not affect any other message routing; there is no need to amend any existing transforms, search rules and so on.

Device provisioning and authentication policy

The Provisioning Server requires that any provisioning or phone book requests it receives have already been authenticated at the zone or subzone point of entry into the VCS. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

The following diagram shows the flow of provisioning messages from an endpoint to the Provisioning Server, together with the credential checking processes:



The VCS must be configured with appropriate device authentication settings, otherwise provisioning-related messages will be rejected:

- Initial provisioning authentication (of a subscribe message) is controlled by the authentication policy setting on the Default Zone. (The Default Zone is used as the device is not yet registered.)
  The Default Zone and any traversal client zone's authentication policy must be set to either *Check credentials* or *Treat as authenticated*, otherwise provisioning requests will fail.
- The authentication of subsequent messages, including registration requests, phone book requests and call signaling messages is controlled by the authentication policy setting on the Default Subzone (or relevant alternative subzone) if the endpoint is registered (which is the usual case), or by the authentication policy setting on the Default Zone if the endpoint is not registered.
  The relevant authentication policy must be set to either *Check credentials* or *Treat as authenticated*, otherwise phone book requests will fail.

In each case, the VCS performs its authentication checking against the appropriate credential store, according to whichever authentication methods are configured. Note that if the VCS is using the local database, this will include all credentials supplied by Cisco TMS.

For more information about provisioning configuration in general, see *Cisco TMS Provisioning Extension Deployment Guide*.

VCS Starter Pack Express

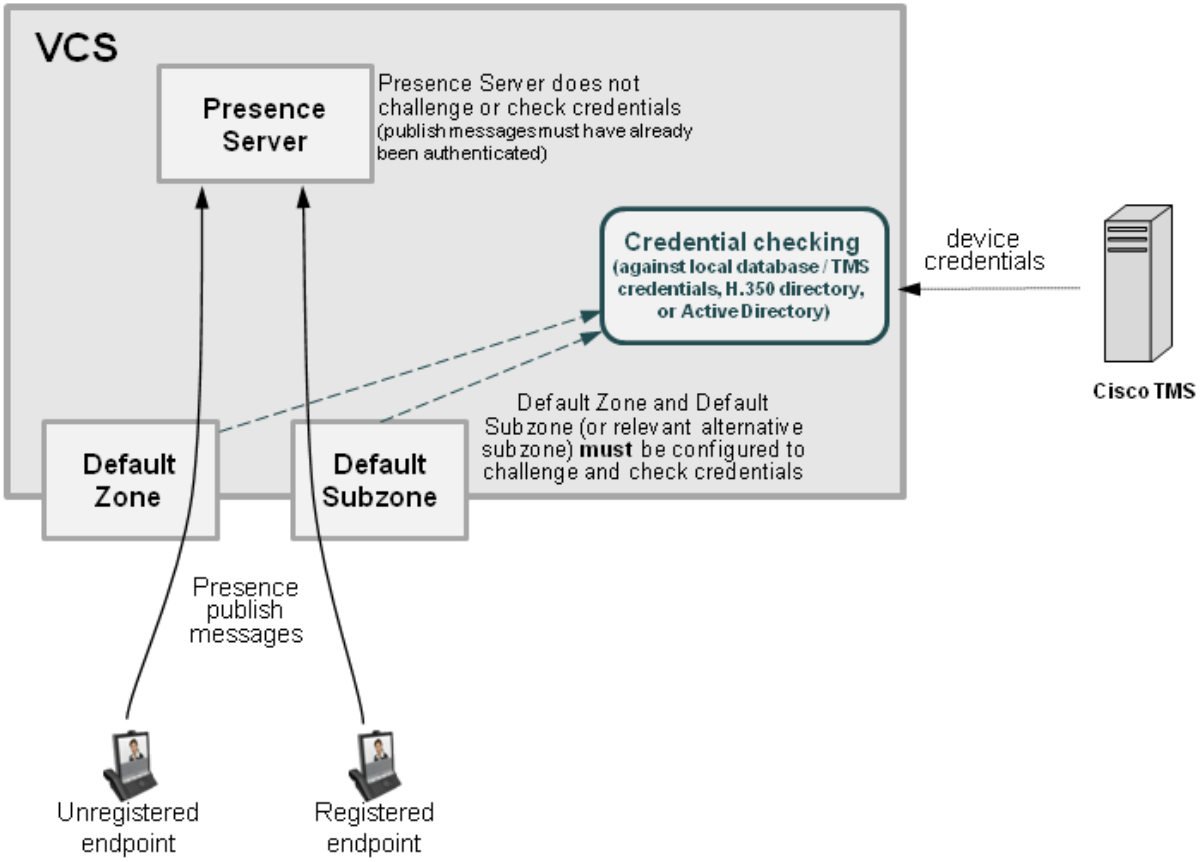
The Provisioning Server on a VCS Starter Pack Express operates in the same manner as when using Cisco TMS provisioning – it does not challenge provisioning requests. It provisions devices only if the request has already been authenticated by the VCS (at the zone or subzone entry point).

Presence and authentication policy

The Presence Server accepts presence PUBLISH messages only if they have already been authenticated:

- The authentication of presence messages by the VCS is controlled by the authentication policy setting on the Default Subzone (or relevant alternative subzone) if the endpoint is registered (which is the usual case), or by the authentication policy setting on the Default Zone if the endpoint is not registered.
- The relevant **Authentication policy** must be set to either *Check credentials* or *Treat as authenticated*, otherwise PUBLISH messages will fail, meaning that endpoints will not be able to publish their presence status.

The following diagram shows the flow of presence messages from an endpoint to the Presence Server:



In each case, the VCS performs its authentication checking against the appropriate credential store, according to whichever authentication methods are configured. Note that if the VCS is using the local database, this will include any credentials supplied by Cisco TMS.

Hierarchical dial plans and authentication policy

Hierarchical dial plan (directory VCS) deployments and device authentication

When introducing authentication into video networks which have a hierarchical dial plan with a directory VCS, authentication problems can occur if:

- any VCS in the network uses a different authentication database from any other VCS in the network, and
- credential checking is enabled on the Default Zone of any VCS (as is needed, for example, when using Cisco TMSPE), and
- the directory VCS or any other VCS in a signaling path can optimize itself out of the call routing path

In such deployments, each VCS must be configured with a neighbor zone between itself and every other VCS in the network. Each zone must be configured with an **Authentication policy** of *Do not check credentials*. (No search rules are required for these neighbor zones; the zones purely provide a mechanism for trusting messages between VCSs.)

This is required because, otherwise, some messages such as SIP RE-INVITES, which are sent directly between VCSs (due to optimal call routing), will be categorized as coming from the Default Zone. The VCS will then attempt to authenticate the message and this may fail as it may not have the necessary credentials in its authentication database. This means that the message will be rejected and the call may be dropped. However, if the node VCSs have a neighbor zone relationship then the message will be identified as coming through that neighbor zone, the VCS will not perform any credential checking (as the neighbor zone is set to *Do not check credentials*) and the message will be accepted.

Deployments with multiple regional / subnetwork directory VCSs

If your deployment is segmented into multiple regional subnetworks, each with their own directory VCS, it is not feasible (or recommended) to set up neighbor zones between each and every VCS across the entire network.

In this scenario you should configure each subnetwork as described above – i.e. set up neighbor zones between each of the VCSs managed by the same directory VCS – and then configure the neighbor zones between each directory VCS so that they stay in the call signaling path on calls crossing subnetworks between those directory VCSs. To do this:

1. On the directory VCS, go to **Configuration > Zones > Zones** and then click on the relevant zone to the other directory VCS.
2. On the **Edit zones** page, scroll down to the **Advanced** section and set **Zone profile** to *Custom*.
3. Set **Call signaling routed mode** to *Always*.
4. Click **Save**.
5. Repeat this for the equivalent zone definition on the “other” directory VCS, and then repeat the entire process for any other zone configurations between any other directory VCSs.

Note: do not modify the directory VCS’s primary **Call signaling routed mode** setting on the **Calls** page.

This means that the each directory VCS will stay in the call signaling path for calls that go between subnetworks. Each directory VCS will still be able to optimize itself out of the call signaling path for calls entirely within each subnetwork.

You must also ensure that you have sufficient call licenses (traversal and non-traversal) on each directory VCS to handle those calls going between each subnetwork.

Practical configuration of authentication policy

VCS Control

The table below contains practical guidelines for configuring authentication policy on a VCS-C.

Authentication point	Guideline
Default Zone	Use *Check credentials*.
Default Subzone	Use *Check credentials*.
Specific local subzones	For known local subnets, to avoid having to configure all local endpoints with credentials, use *Treat as authenticated*. Although this is a practical solution, we recommend that no *Treat as authenticated* subzones are used, and that every endpoint is populated with appropriate and unique credentials and that *Check credentials* is used.
Other subzones	Use *Check credentials*.
Traversal zone	Use *Check credentials*. Always check the credentials of requests coming from the VCS Expressway.
Neighbor zone	Use *Do not check credentials* and set **SIP authentication trust mode** to *On*.

VCS Expressway

Ideally, VCS Expressway authentication policy, should follow exactly the same guidelines as for the VCS Control. However if AD Direct or H.350 access is required, many security policies will not allow a device in a DMZ access to those resources. Practicality therefore recommends that authentication is left to the VCS Control. For SIP devices you can use delegated credential checking; this allows SIP devices to register to the VCS Expressway but be authenticated via a device authentication mechanism configured on the VCS Control.

You can also use registration allow and deny lists to limit what can register to the VCS Expressway. If it is required that outbound calls may only be made by authenticated users, ensure that all call requests are routed to the VCS Control and it only forwards requests back that it can authenticate.

Infrastructure devices

You are recommended to configure your VCS so that infrastructure products, such as MCUs, register to a dedicated subzone with an authentication policy set to *Treat as authenticated*.

Authentication methods

Configuring VCS authentication methods

The VCS supports 3 different methods of verifying authentication credentials:

- against an on-box local database (which includes any Cisco TMS-supplied credentials)
- via an LDAP connection to an external H.350 directory service
- via direct access to an Active Directory server using a Kerberos connection (NTLM challenges only)

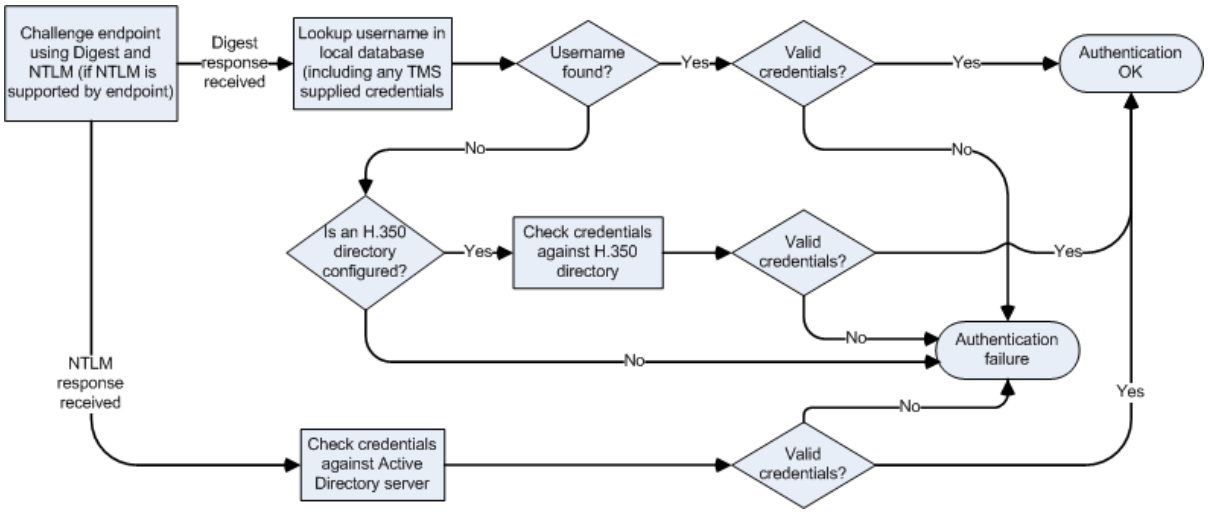
The VCS attempts to verify the credentials presented to it by first checking against its on-box local database of usernames and passwords. The local database also includes checking against credentials supplied by Cisco TMS if your system is using device provisioning. If the username is not found in the local database, the VCS may then attempt to verify the credentials via a real-time LDAP connection to an external H.350 directory service. The directory service, if configured, must have an H.350 directory schema for either a Microsoft Active Directory LDAP server or an OpenLDAP server.

Along with one of the above methods, for those devices that support NTLM challenges, the VCS can alternatively verify credentials via direct access to an Active Directory server using a Kerberos connection. The direct Active Directory authentication via Kerberos method is only supported by a limited range of endpoints – at the time of writing, only Cisco Jabber for iPad and Jabber Video. If used, other non-supported endpoint devices will continue to authenticate using one of the other two authentication methods.

Note that the VCS always challenges an endpoint with a standard Digest challenge. The VCS will additionally send an NTLM challenge if the VCS has NTLM protocol challenges enabled and it recognizes that the endpoint supports NTLM.

If the endpoint receives both challenges, it is the endpoint's decision as to whether to respond to the Digest challenge or to the NTLM challenge. At the time of writing, all supported endpoints respond to an NTLM challenge in preference to a Digest challenge.

The following diagram shows the process followed by the VCS when authenticating credentials:



Note that accurate timestamps play an important part in authentication of H.323 devices, helping to guard against replay attacks. For this reason, if you are using device authentication with H.323 devices, both the VCS and the endpoints must use an NTP server to synchronize their system time.

Authentication mechanism

The authentication process uses a username and password-based challenge-response scheme to check a device's credentials.

The actual mechanism used by the device to supply its credentials to the VCS depends on the protocol being used:

- **H.323**: any necessary credentials are contained within the incoming request. (The VCS supports the *ITU H.235 specification* for authenticating the identity of H.323 network devices with which it communicates.)
- **SIP**: credentials are not contained within the initial request. Instead the VCS sends a challenge back to the sender that asks for its credentials. However, if a SIP message has already been authenticated (for example by another VCS on a previous hop), that system may insert information into the SIP message to show that it has been authenticated. You can control whether the VCS chooses to trust any authentication carried out at an earlier stage by configuring a zone's SIP authentication trust setting.

Note that if the VCS is acting as a traversal server, you must ensure that each traversal client's authentication credentials are entered into the selected database.

Endpoint credentials used for authentication

An endpoint must supply the VCS with a username and password if it is required to authenticate with the VCS, for example when attempting to register and the relevant subzone's **Authentication policy** is set to *Check credentials*.

For Cisco endpoints using H.323, the username is typically the endpoint's **Authentication ID**; for Cisco endpoints using SIP it is typically the endpoint's **Authentication username**.

See the relevant endpoint manual for details about how to configure the endpoint's credentials.

Configuring authentication to use the local database

The local authentication database is included as part of your VCS system and does not require any specific connectivity configuration. It is used to store user account authentication credentials. Each set of credentials consists of a **name** and **password**.

The credentials in the local database can be used for device (SIP and H.323), traversal client and TURN client authentication.

Adding credentials to the local database

To enter a set of device credentials:

1. Go to **Configuration > Authentication > Devices > Local database** and click **New**.
2. Enter the **Name** and **Password** that represent the device's credentials.
3. Click **Create credential**.

Note that the same credentials can be used by more than one device.

Credentials managed within Cisco TMS (for device provisioning)

When the VCS is using TMS Provisioning Extension services, the credentials supplied by the Users service are stored in the local authentication database, along with any manually configured entries. The **Source** column identifies whether the user account name is provided by **TMS**, or is a **Local** entry. Only **Local** entries can be edited.

Incorporating Cisco TMS credentials within the local database means that VCS can authenticate all messages (i.e. not just provisioning requests) against the same set of credentials used within Cisco TMS.

Local database authentication in combination with H.350 directory authentication

You can configure the VCS to use both the local database and an H.350 directory.

If an H.350 directory is configured, the VCS will always attempt to verify any Digest credentials presented to it by first checking against the local database before checking against the H.350 directory.

Local database authentication in combination with Active Directory (direct) authentication

If Active Directory (direct) authentication has been configured and NTLM protocol challenges is set to Auto, then NTLM authentication challenges are offered to those devices that support NTLM.

- NTLM challenges are offered in addition to the standard Digest challenge.
- Endpoints that support NTLM will respond to the NTLM challenge in preference to the Digest challenge, and the VCS will attempt to authenticate that NTLM response.

Starter Pack

If the **Starter Pack** option key is installed, the local authentication database will include a pre-configured set of authentication credentials. To ensure correct operation of the TURN server in conjunction with the Starter Pack, do not delete or modify the **StarterPackTURNUser** entry in the local authentication database.

All other credentials that are required to support Starter Pack provisioned devices have to be added manually for each user account.

Using an H.350 directory service lookup via LDAP

The **Device authentication H.350 configuration** page (**Configuration > Authentication > Devices > H.350 directory service**) is used to configure a connection via LDAP to an H.350 directory service. An H.350 directory service lookup can be used for authenticating any endpoint, SIP and H.323.

H.350 directory authentication and registration process

If the VCS is using an H.350 directory service to authenticate registration requests, the process is as follows:

1. The endpoint presents its username and authentication credentials to the VCS, and the aliases with which it wants to register.
2. The VCS then determines which aliases the endpoint is allowed to attempt to register with, based on the **Source of aliases for registration** setting. For H.323 endpoints, you can use this setting to override the aliases presented by the endpoint with those in the H.350 directory, or you can use them in addition to the endpoint's aliases. For SIP endpoints, you can use this setting to reject a registration if the endpoint's AOR does not match that in the H.350 directory. The options are:
   - *H.350 directory*: for SIP registrations the AOR presented by the endpoint is registered providing it is listed in the H.350 directory for the endpoint's username.
     For H.323 registrations:
     - At least one of the aliases presented by the endpoint must be listed in the H.350 directory for that endpoint's username. If none of the presented aliases are listed it is not allowed to register.
     - The endpoint will register with all of the aliases (up to a maximum of 20) listed in the H.350 directory. Aliases presented by the endpoint that are not in the H.350 directory will not be registered.
     - If no aliases are listed in the H.350 directory, the endpoint will register with all the aliases it presented.
     - If no aliases are presented by the endpoint, it will register with all the aliases listed in the H.350 directory for its username.
   - *Combined*: the aliases presented by the endpoint are used in addition to any listed in the H.350 directory for the endpoint's username. In other words, this is the same as for *H.350 directory*, except that if an endpoint presents an alias that is not in the H.350 directory, it will be allowed to register with that alias.
   - *Endpoint*: the aliases presented by the endpoint are used; any in the H.350 directory are ignored. If no aliases are presented by the endpoint, it is not allowed to register.

   The default is *H.350 directory*.

Note that if the authentication policy is *Do not check credentials* or *Treat as authenticated*, then the **Source of aliases for registration** setting is ignored and the aliases presented by the endpoint are used.

Configuring the LDAP server directory

The H.350 directory on the LDAP server should be configured to implement the *ITU H.350 specification*. it should store credentials for devices with which the VCS communicates, and the aliases of endpoints that will register with the VCS.

1. Download the required H.350 schemas from the VCS (**Configuration > Authentication > Devices > H.350 directory schemas**) and install them on the LDAP server.
2. Configure the directory with the aliases of endpoints that will register with the VCS.

Configuring the LDAP server settings

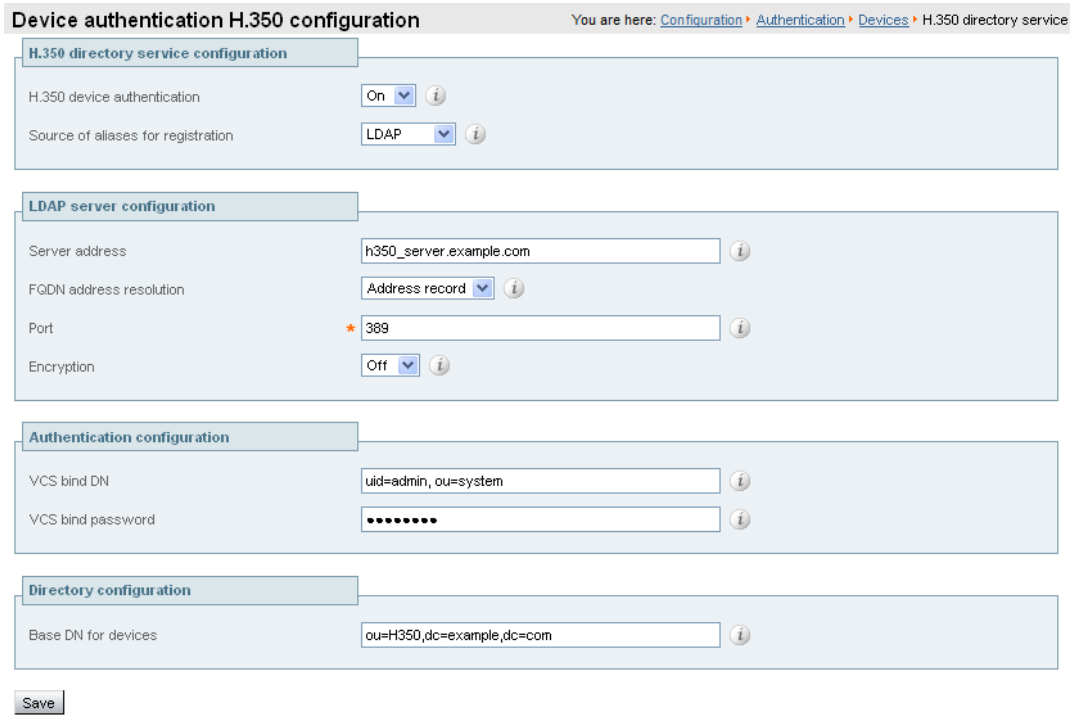
1. Go to **Configuration > Authentication > Devices > H.350 directory service**.

2. Configure the fields as follows:

H.350 device authentication	Select *On*.	The H.350 directory can be used in combination with other authentication mechanisms.
Source of aliases for registration	Determines how aliases are checked and registered.	See **H.350 directory authentication and registration process** above for a description of each setting. When **Source of aliases for registration** is *H.350 directory*, MCUs are treated as a special case. They register with the presented aliases and ignore any aliases in the H.350 directory. (This is to allow MCUs to additively register aliases for conferences.)
Server address	The IP address or FQDN (or server address, if a DNS **Domain name** has also been configured) of the LDAP server.	The LDAP server must have the H.350 schemas installed.
FQDN address resolution	Defines how the LDAP **Server address** is resolved if it is specified as an FQDN. *Address record*: DNS A or AAAA record lookup. *SRV record*: DNS SRV record lookup.	DNS SRV lookups enable the VCS to authenticate devices against multiple remote H.350 directory servers. This provides a seamless redundancy mechanism in the event of reachability problems to an H.350 directory server. The SRV lookup is for either _ldap._tcp or _ldap._tls records, depending on whether **Encryption** is enabled. If multiple servers are returned, the priority and weight of each SRV record determines the order in which the servers are used.
Port	The IP port of the LDAP server.	Typically, non-secure connections use *389* and secure connections use *636*.
Encryption	Determines whether the connection to the LDAP server is encrypted using Transport Layer Security (TLS). *TLS*: uses TLS encryption for the connection to the LDAP server. *Off*: no encryption is used.	When TLS is enabled, the LDAP server's certificate must be signed by an authority within the VCS's trusted CA certificates file. Click **Upload a CA certificate file for TLS** (in the **Related tasks** section) to go to the **Trusted CA certificate** page.
Bind DN	The user distinguished name used by the VCS when binding to the LDAP server.	For example, uid=admin, ou=system
Bind password	The password used by the VCS when binding to the LDAP server.	
Base DN for devices	The area of the directory on the LDAP server to search for credential information. This should be specified as the Distinguished Name (DN) in the LDAP directory under which the H.350 objects reside.	For example, ou=H350,dc=example,dc=com

3. Click **Save**.

The current status of the connection to the specified LDAP server is displayed at the bottom of the page.



Using an H.350 directory with other authentication mechanisms

Local database authentication in combination with H.350 directory authentication

You can configure the VCS to use both the local database and an H.350 directory.

If an H.350 directory is configured, the VCS will always attempt to verify any Digest credentials presented to it by first checking against the local database before checking against the H.350 directory.

H.350 directory service authentication in combination with Active Directory (direct) authentication

If Active Directory (direct) authentication has been configured and **NTLM protocol challenges** is set to *Auto*, then NTLM authentication challenges are offered to those devices that support NTLM. Devices that do not support NTLM will continue to receive a standard Digest challenge.

Using Active Directory database (direct)

Active Directory database (direct) authentication uses NTLM protocol challenges and authenticates credentials via direct access to an Active Directory server using a Kerberos connection.

It can be enabled at the same time as local database and H.350 directory service authentication. This is because NTLM authentication is only supported by certain endpoints. Therefore, for example, you could use the Active Directory (direct) server method for Jabber Video, and the local database or H.350 directory service authentication for the other devices that do not support NTLM.

If Active Directory (direct) authentication has been configured and **NTLM protocol challenges** is set to *Auto*, then NTLM authentication challenges are offered to those devices that support NTLM. Devices that do not support NTLM will continue to receive a standard Digest challenge.

Configuration prerequisites

Active Directory

- A username and password of an AD user account with either “account operator” or “administrator” access rights must be available for the VCS to use for joining and leaving the domain.
- Entries must exist in the Active Directory server for all devices that are to be authenticated through this method. Each entry must have an associated password.
- The device entries (in all domains) must be accessible by the user account that is used by VCS to join the domain. If the VCS is in a domain that is part of a forest, and there is trust between domains in the forest, the VCS can authenticate device entries from different domains providing the user account has appropriate rights to authenticate devices against the other domains.

Kerberos Key Distribution Center

The KDC (Kerberos Key Distribution Center) server must be synchronized to a time server.

DNS server

If a DNS name or DNS SRV name is used to identify the AD servers, a DNS server must be configured with the relevant details. (Note that the VCS must be configured to use a DNS server even if you are not using DNS / DNS SRV to specify the AD servers.)

VCS

- The VCS must be configured to use a DNS server (**System > DNS**).
  - The VCS’s **System host name** (**System > DNS**) must be 15 or fewer characters long. (Microsoft NetBIOS names are capped at 15 characters.)
  - When part of a cluster, ensure that each VCS peer has a unique **System host name**.
- Ensure that an NTP server (**System > Time**) has been configured and is active.
- If the connection is going to use TLS encryption, a valid CA certificate, private key and server certificate must be uploaded to the VCS.
- The VCS must be configured to challenge for authentication on the relevant zones and subzones:
  - The Default Zone (**Configuration > Zones > Zones**, then select Default Zone) must be configured with an **Authentication policy** of *Check credentials*. This ensures that provisioning requests (and any call requests from non-registered devices) are challenged.
  - The Default Subzone (**Configuration > Local Zone > Default Subzone**) – or the relevant subzones - must be configured with an **Authentication policy** of *Check credentials*. This ensures that registration,

presence, phone book and call requests from registered devices are challenged.

Setting up your authentication policy to check credentials will affect any device that sends provisioning, registration, presence, phone book and call requests to the VCS.

Endpoint

The PC on which Jabber Video runs must use settings which match the settings of the AD server.

Configuring the connection to Active Directory Service (ADS)

The **Active Directory Service** page (**Configuration > Authentication > Devices > Active Directory Service**) is used to configure a connection to an Active Directory Service for device authentication of Jabber Video endpoints (version 4.2 or later).

Configuring the Active Directory Service settings

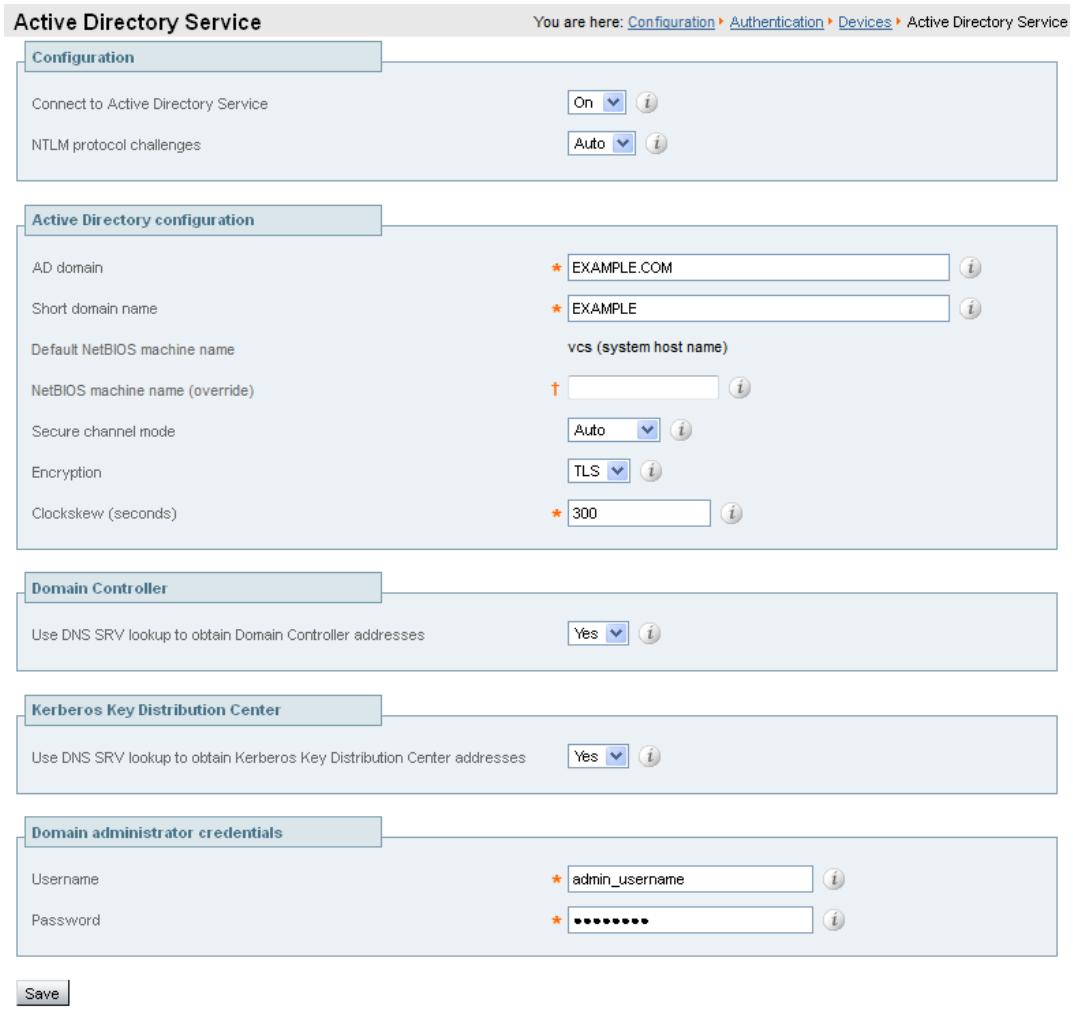
To configure Active Directory (direct) and join the AD domain:

1. Go to **Configuration > Authentication > Devices > Active Directory Service**.
2. Configure the fields as follows:

Connect to Active Directory Service	Select *On*.	Turning **Connect to Active Directory Service** to *Off* does not cause the VCS to leave the AD domain.
NTLM protocol challenges	Controls whether or not the VCS sends NTLM protocol challenges (in addition to Digest challenges) when authenticating devices over SIP. *Auto*: the VCS decides, based on the device type, whether to send NTLM challenges. *Off*: NTLM challenges are never sent. *On*: NTLM challenges are always sent. The default is *Auto*.	Normally, this should be set to *Auto*. If you are migrating from an existing authentication mechanism to ADS then select *Off* while the connection to the AD server is being configured; select *Auto* later, when you have an active connection and are ready to switch over to this authentication mechanism. Never use *On*, as this will send NTLM challenges to devices that may not support NTLM (and therefore they may crash or otherwise misbehave). The VCS must be connected to an Active Directory Service to send NTLM challenges.
AD domain	This must be the fully qualified domain name (FQDN) of the AD domain that the VCS will join. It must be entered in upper case, such as, EXAMPLE.COM.	Typically the domain is the same as the DNS name of the Kerberos server. Upper case entry is enforced due to case sensitivity issues with Active Directory.
Short domain name	The short domain name used by the VCS when it joins the AD domain.	It is also known as the NetBIOS domain name.

NetBIOS machine name (override)	By default the system uses the **System host name** as the NetBIOS machine name when joining the AD domain. If required, you can enter a different name here to override the default name.	An override must be specified if the **System host name** exceeds 15 characters.
Secure channel mode	Indicates if data transmitted from the VCS to an AD Domain Controller is sent over a secure channel. *Auto*: automatically adapts to the domain controller's settings. *Enabled*: always attempts to use a secure channel. *Disabled*: does not use a secure channel. The default is *Auto*.	You are recommended to use *Auto*.
Encryption	Sets the encryption to use for the LDAP connection to the Active Directory Service. *Off*: no encryption is used. *TLS*: TLS encryption is used. The default is *TLS*.	If encryption is set to TLS, a valid CA certificate, private key and server certificate must be uploaded to the VCS. Click **Upload a CA certificate file for TLS** (in the **Related tasks** section) to go to the Trusted CA certificate page.
Clockskew	The maximum allowed clockskew (in seconds) between the VCS and the KDC before the Kerberos message is assumed to be invalid. The default is 300 seconds.	It should be kept in step with the clock skew setting on the KDC. Ensure that VCS and KDC are synchronized to time servers.
Use DNS SRV lookup to obtain Domain Controller addresses	*Yes* is the recommended setting. This means that VCS will use a DNS SRV lookup of the **AD domain** to obtain the address details of the AD domain controllers. If the lookup cannot provide the addresses then set this field to *No* and enter the IP address of the primary Domain Controller into the **Address 1** field that will be displayed.	
Use DNS SRV lookup to obtain Kerberos Key Distribution Center addresses	*Yes* is the recommended setting. This means that VCS will use a DNS SRV lookup of the **AD domain** to obtain the address details of the Kerberos Key Distribution Center servers. If the lookup cannot provide the addresses then set this field to *No* and enter the IP address of the primary Key Distribution Center servers into the **Address 1** field that will be displayed. Typically, **Port 1** can be left as its default value of 88.	Typically, the KDC addresses are the same as the Domain Controller addresses.
Username and **Password**	The AD domain administrator username and password. The password is case sensitive.	The domain administrator's credentials are required only when you attempt to join a domain. The VCS only needs to join the domain once, after which the connection can be enabled or disabled as required.

3. Click **Save** to store the configuration and join the AD domain.
   The VCS should join the AD domain. If you receive an error message, check the following:
   - the configuration settings on this page, including the username and password
   - the VCS's CA certificate, private key and server certificate
   - the **Status** area at the bottom of the Active Directory Service page for more information about the status of the connection to the AD domain



Note that:

- The domain administrator username and password are not stored in VCS; they are only required to join an AD domain (or to leave a domain).
- The VCS only needs to join the AD domain once, even if the connection to the Active Directory Service is disabled and turned back on again. The only time a join is needed again is if the VCS leaves the domain or needs to join a different domain.

Adding non-primary Domain Controllers and Kerberos Key Distribution Center servers (optional)

This procedure is only required if you are not using DNS SRV lookups of the **AD domain** to obtain the address details of the Domain Controller servers and the Kerberos Key Distribution Center servers.

1. Go to **Configuration > Authentication > Devices > Active Directory Service**.
2. Enter up to 4 further Domain Controller server addresses (up to 5 in total).
3. Enter up to 4 further Kerberos Key Distribution Center server addresses and port numbers (up to 5 in total).
4. Click **Save**.
5. If the VCS is part of a cluster, check that the configuration entered on the master peer has been replicated to each other peer.

Clustered VCS systems

In a clustered system, each VCS must join the AD domain separately. To do this:

On the master peer:

1. Follow the instructions as above to configure Active Directory (direct) and join the AD domain.
2. Ensure that the master peer has successfully joined the AD domain before continuing.

On each other peer in turn:

1. Go to **Configuration > Authentication > Devices > Active Directory Service**.
2. Check that the configuration entered on the master peer has been replicated to the current peer.
3. Enter the AD domain administrator **Username** and **Password**.
   (These credentials are not stored by the VCS and so have to be entered each time.)
4. Click **Save**.
   The VCS should join the AD domain. If you receive an error message, check the following:
   - the configuration settings on this page, including the username and password
   - the VCS's CA certificate, private key and server certificate (CA certificate information is not replicated across cluster peers)

Enabling NTLM authentication challenges

When Active Directory details have been configured and the VCS has been joined into the AD domain, VCS can now be configured to challenge Jabber Video (4.2 or later) with NTLM authentication challenges.

1. Go to **Configuration > Authentication > Devices > Active Directory Service**.
2. Ensure that **NTLM protocol challenges** is set to *Auto*.
   Never use *On*, as this will send NTLM challenges to devices that may not support NTLM (and therefore they may crash or otherwise misbehave).
3. Click **Save** if required.
4. If the VCS is part of a cluster, check that any configuration changes entered on the master peer have been replicated to each other peer.

Configuring Jabber Video and testing Active Directory database (direct) authentication

We recommend that you use a Jabber Video configuration that already authenticates successfully using either provisioning or VCS authentication. This means that Jabber Video's Advanced settings (**Internal Server**, **External Server** and **SIP Domain** entries) are correctly configured.

1. Sign in to Jabber Video:
2. In the **Username** field, configure **`<AD Short Domain Name>\username`**

(this field is not case sensitive).

3. In the **Password** field, enter the password as configured in the Active Directory database for the chosen user.
4. Click **Sign in**.

A successful registration confirms that authentication of provisioning and registration of Jabber Video to VCS now works using Active Directory database (direct) authentication.

Ports

See Device authentication port reference [p.36] for a list of ports used when communicating with the AD system.

Authenticating with external systems

The **Outbound connection credentials** page (**Configuration > Authentication > Outbound connection credentials**) is used to configure a username and password that the VCS will use whenever it is required to authenticate with external systems.

For example, when the VCS is forwarding an invite from an endpoint to another VCS, that other system may have authentication enabled and will therefore require your local VCS to provide it with a username and password.

Note that these settings are not used by traversal client zones. Traversal clients, which must always authenticate with traversal servers before they can connect, configure their connection credentials per traversal client zone.

Appendix 1: Troubleshooting

This section provides information to help troubleshoot and resolve authentication issues.

Local database troubleshooting

No specific troubleshooting.

H.350 directory service troubleshooting

No specific troubleshooting.

Active Directory (direct) troubleshooting

Check password

If it is a device specific entry, check that the password has been activated and has not expired.

If it is a user login, check that the user can use the username and password in a different application.

Jabber Video fails to authenticate

Mismatch of NTLM versions

To use Active Directory (direct) mode, the PC running Jabber Video must use appropriate settings which are compatible with the AD server. To check (and change if required), see "Jabber Video PC and AD server compatibility configuration [p.41]".

Username too long

The Jabber Video username must not exceed 20 characters. Usernames longer than 20 characters will fail to log in due to a limitation in Active Directory which truncates longer names.

Netlogon Log Error Codes - NTreasonCodes

In a diagnostic log taken of an AD direct authentication, NT supplied reason code values are returned in failure cases. The log contains: NTreasonCode="<value>"; these values are documented at: http://technet.microsoft.com/en-us/library/cc776964%28v=ws.10%29.aspx. In summary:

Log Code	Description
0x0	Successful login
0xC0000022	Domain controller is denying access (try joining domain again)
0xC0000064	The specified user does not exist (user name does not exist)
0xC000006A	The value provided as the current password is not correct (name is correct but the password is wrong)
0xC000006C	Password policy not met
0xC000006D	The attempted logon is invalid due to a bad user name

Log Code	Description
0xC000006E	User account restriction has prevented successful login
0xC000006F	The user account has time restrictions and may not be logged onto at this time (user tried to logon outside his day of week or time of day restrictions)
0xC0000070	The user is restricted and may not log on from the source workstation
0xC0000071	The user account's password has expired
0xC0000072	The user account is currently disabled
0xC000009A	Insufficient system resources
0xC0000133	Clocks between DC and other computer too far out of sync
0xc000015b	The user has not been granted the requested logon type (aka logon right) at this machine
0xC0000193	The user's account has expired
0xC0000224	User must change his password before he logs on
0xC0000234	The user account has been automatically locked (user is currently locked out)

PC fails to login after a video endpoint has had AD direct authentication login failures

If the AD Authentication has a limit to the number of failed logins that are allowed, failed logins from an endpoint will affect authentication of anything else that uses AD to authenticate.

Device provisioning (TMSPE mode) and presence

SUBSCRIBE for provisioning rejected / provisioned endpoint cannot sign in

- Check that the Default Zone is configured with an **Authentication policy** of *Check credentials* or *Treat as authenticated*.

SUBSCRIBE for provisioning and Jabber Video sign ins will fail if the **Authentication policy** is *Do not check credentials*.

If authentication is set to *Check credentials* (recommended) the appropriate username and password must be configured in the relevant credential database.

- Check that the account username, the authentication credential name, and the Jabber Video sign in username all match (note that from X7.1 and later, usernames are case insensitive).

If the Jabber Video sign in username and the authentication credential name do not match then the initial Subscribe will be rejected as unauthorized.

If the Jabber Video sign in username and the account username do not match then the Subscribe is authenticated but the Notify is sent with Reason: rejected; Content length: 0.

Phone book searches do not return any entries

Phone book search requests are rejected if the Default Subzone is configured with an **Authentication policy** of *Do not check credentials*.

- We recommended that you set the Default Subzone authentication to *Check credentials* and configure the appropriate usernames and passwords in the relevant credential database.

Failed to update presence

Jabber Video displays a “Failed to update Presence” message if the Default Subzone is configured with an **Authentication policy** of *Do not check credentials*.

- We recommended that you set the Default Subzone authentication to *Check credentials* and configure the appropriate usernames and passwords in the relevant credential database.

Appendix 2: Additional information

Device authentication port reference

H.350 directory service

The following table lists the ports used for device authentication between VCS and the H.350 server. They are configurable via **Configuration > Authentication > Devices > H.350 directory service**.

Purpose	VCS port	Destination port
H.350 LDAP server	TCP ephemeral port	TCP/389 or TCP/636

Active Directory (direct)

The following table lists the ports used for device authentication between VCS and the AD system. They are configurable via **Configuration > Authentication > Devices > Active Directory Service**.

Purpose	VCS port	Destination port
Kerberos Key Distribution Center	UDP ephemeral port	88 UDP
Kerberos	TCP ephemeral port	88 TCP
VCS with Domain Controller (CLDAP)	UDP ephemeral port	389 UDP
VCS with Domain Controller (LDAP)	TCP ephemeral port	389 / 636 TCP
Client credential authentication with the Domain Controller (Microsoft-DS). VCS initially tries port 445, but if that cannot be reached it tries port 139.	TCP ephemeral port	445 / 139 TCP

Certificates for TLS

For the VCS to connect to a server over TLS, the trusted CA certificate installed on the VCS must be able to authorize that server's server certificate.

For more information see *Certificate Creation and Use with VCS Deployment Guide*.

Use with VCS clusters

Active Directory (direct)

All authentication configuration is replicated across cluster peers, however the DNS server is configurable independently on each VCS peer. Make sure that each peer references a DNS server that can look up the AD server, Kerberos KDC and other required DNS and DNS SRV addresses.

Joining or leaving a domain must be carried out for every peer of the cluster, as each peer independently connects to the AD server.

IT requisition

H.350 directory service: IT requisition (for LDAP access to H.350 directory service)

To: IT Department

Please supply the following details so that the VCS can be configured to authenticate video endpoint calls using LDAP access to the H.350 directory service server.

LDAP Server IP or domain	
IP port for LDAP access	389 / 636 / Other:
Encryption	Off / TLS
Distinguished name of username used when binding to the H.350 LDAP server (e.g. uid=, ou=)	
Password to use when binding to the H.350 LDAP server	
Distinguished name to use when connecting to the H.350 LDAP server (e.g. ou=,dc=)	

Active directory (direct): IT requisition (for access to Active Directory server)

To: IT Department

Please supply the following details so that the VCS can be configured to access the Active Directory server to authenticate video endpoint calls.

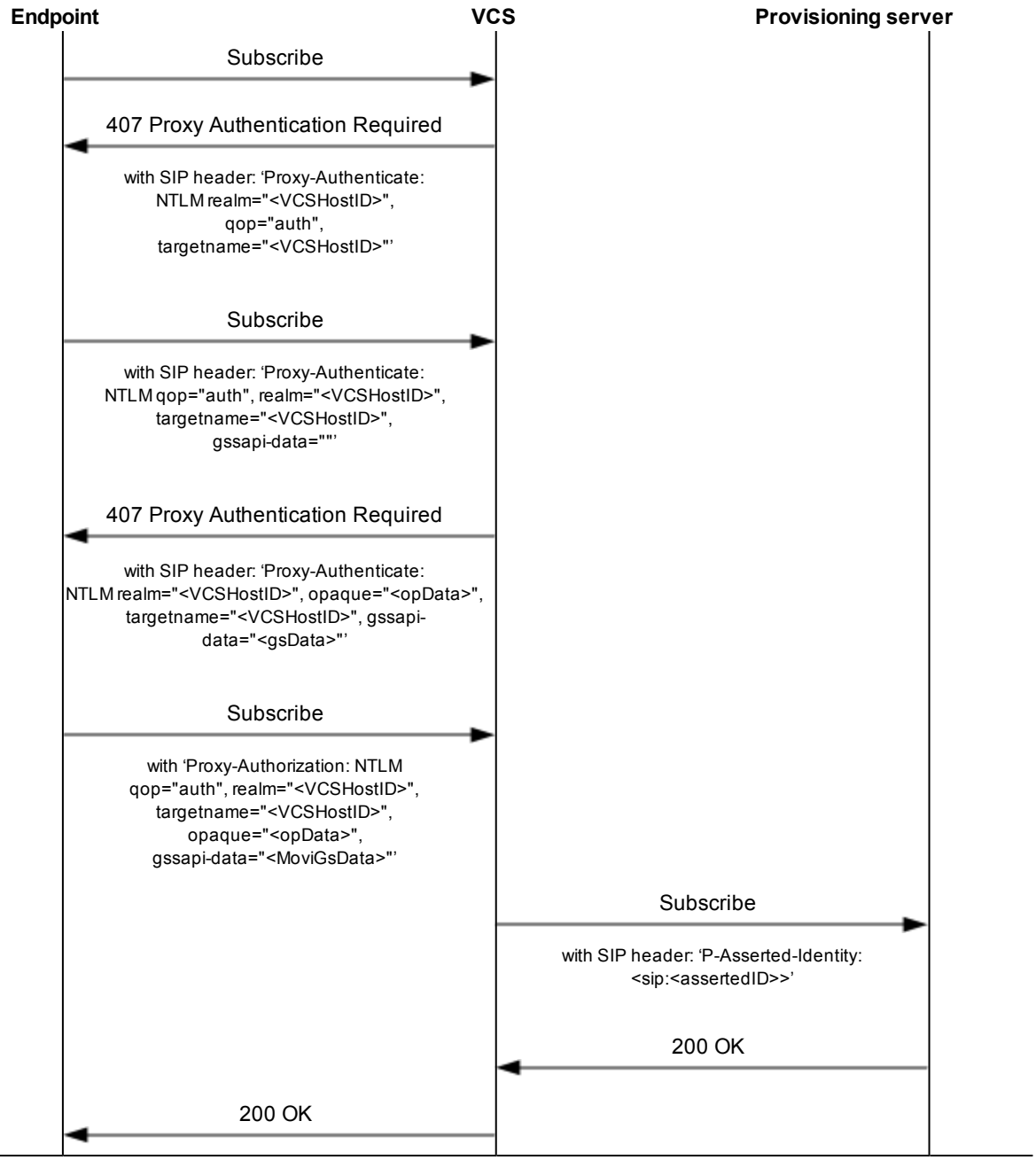
Active Directory Domain (FQDN)	
Active Directory Short Domain Name (NetBIOS Domain Name)	
Is a secure channel required between VCS and the AD domain controller?	YES / NO
Is TLS encryption needed between VCS and the AD server? Certificate location?	YES / NO Path to certificate file:
Is a clock skew value other than 300 (5 mins) required between the VCS and the Kerberos Key Distribution Center?	300 (default) / Other:
Is SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) used to identify appropriate authentication protocols between VCS and the AD domain controller?	YES / NO
Domain Controller servers Are these available by a DNS SRV lookup to **`_ldap._tcp.dc._msdcs.<Domain>`** If not, specify the IPs of the DC servers:	 YES / NO 1. 2. 3. 4. 5.
Kerberos Key Distribution Center servers Are these available by DNS SRV lookups to **`_kerberos._udp.<Domain>`** and **`_kerberos._tcp.<Domain>`** If not, specify the IPs of KDC servers:	 YES / NO 1. 2. 3. 4. 5.
Administrator username (used for joining the VCS to the domain)	
Administrator password (used for joining the VCS to the domain)	

Appendix 3: Active Directory (direct)

SIP messages for a provisioning subscription

The ladder diagram below shows the call flow for SIP messaging when authentication is challenged using NTLM (Active Directory direct).

The provisioning server may reside on the VCS which authenticates the messaging – in which case the destination of the signaling will be seen as 127.0.0.1, alternatively the messages may be sent to a different VCS (for example, a VCS Control from a VCS Expressway) where the provisioning server resides.



Example DNS SRV configuration for AD

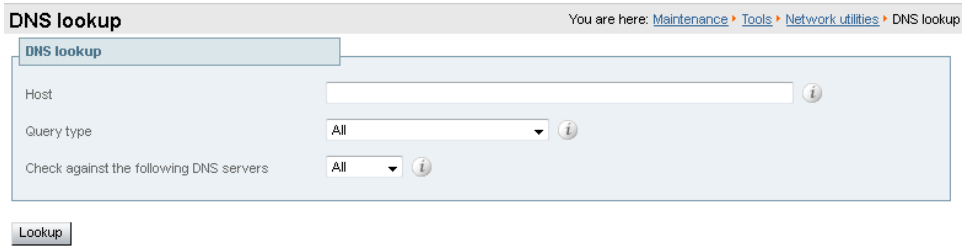
Expected DNS SRV values

The VCS will expect to find the following DNS SRV records. DNS SRV records are set up automatically by the AD server if it can access the DNS server.

SRV lookup	Comment
_ldap._tcp.dc._msdcs.<Domain>	Provides the address of the Domain Controller for the domain.
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.<Domain>	Provides the first site name.
_kerberos._udp.<Domain>	Provides the KDC server address for access via UDP. This entry must list port 88 for each KDC.
_kerberos._tcp.<Domain>	Provides the KDC server address for access via TCP. This entry must list port 88 for each KDC.
_ldap._tcp.<Domain>	Provides the LDAP service on the Domain Controller. This record must list port 389 for the DC.

Checking DNS SRV settings

1. Go to **Maintenance > Tools > Network utilities > DNS lookup**.
2. Enter the SRV path in the **Host** field.
3. Click **Lookup**.



Checking DNS SRV settings (Dig command)

Presence of the correct DNS entries can be validated by executing:

```
root#  dig <DNS server> -t any <full dnssrv record, e.g. _ldap._tcp.dc._msdcs.<DOMAIN>>
```

Example response:

```
; <<>> DiG 9.4.1 <<>> <DNS server> -t any <full dnssrv record>
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44952
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2
```

```
;; QUESTION SECTION:
; <full dnssrv record>.       IN      ANY

;; ANSWER SECTION:
<full dnssrv record>. 600     IN      SRV     0 100 389 <A record 1>.
<full dnssrv record>. 600     IN      SRV     1 100 389 <A record 2>.

;; ADDITIONAL SECTION:
<A record 1>.         3600    IN      A       <IP address 1>
<A record 1>.         1200    IN      A       <IP address 2>

;; Query time: 0 msec
;; SERVER: <DNS server>#53(10.1.1.16)
;; WHEN: Mon Jul 26 11:09:59 2010
;; MSG SIZE  rcvd: 171
~ #
```

Jabber Video PC and AD server compatibility configuration

LMCompatibility level for Jabber Video and the AD server

LMCompatibility level is set both on clients (e.g. Jabber Video PC) and the Domain Controller hosting the Active Directory server. It is important that the values selected on the Jabber Video PC are compatible with the value set on the AD database Domain Controller.

The meanings of the values in LmCompatibilityLevel are explained in http://technet.microsoft.com/en-us/library/cc960646.aspx but in summary are:

Jabber Video client PC

	Client sends:			
Level	**LM**	**NTLM**	**NTLM 2**	**NTLM2 security (if negotiated)**
0	✓	✓	-	-
1	✓	✓	-	✓
2	-	✓	-	✓
3	-	-	✓	✓
4	-	-	✓	✓
5	-	-	✓	✓

AD Domain Controller

	DC accepts:		
Level	**LM**	**NTLM**	**NTLM 2**
0	✓	✓	✓
1	✓	✓	✓

Level	DC accepts: LM	NTLM	NTLM 2
2	✓	✓	✓
3	✓	✓	✓
4	-	✓	✓
5	-	-	✓

Compatibilities

AD Domain Controller Level	Jabber Video client PC
0, 1, 2, 3, 4	0, 1, 2, 3, 4, 5
5	3, 4, 5

The setting called “LmCompatibilityLevel” can be found in the Windows registry.

Using regedit, go to My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

The key is called LmCompatibilityLevel (REG_DWORD)

NtlmMinClientSec and session security level

Microsoft supports different versions of session security in NTLM v2.

Enhanced session security is not supported by VCS prior to X7.1, and if selected on a client when using a VCS version prior to X7.1 authentication will fail.

The session security level is controlled by the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA\MSV1_0\NtlmMinClientSec
```

On VCS prior to X7.1, if NtlmMinClientSec is set to mandate "NTLM 2 session security" Jabber Video authentication will fail.

Recommended client setting for use with VCS software X7.1 and later:

```
LmCompatibilitylevel set to 3, 4 or 5
NtlmMinClientSec set to 0x20080000
```

With the above settings, the Jabber Video client will use NTLMv2 with 128-bit encrypted NTLM 2 session security.

From Microsoft:

```
Value: NtlmMinClientSec
Value Type: REG_DWORD - Number
Valid Range: the logical 'or' of any of the following values:
   0x00000010
   0x00000020
   0x00080000
   0x20000000
Default: 0
```

```
Value: NtlmMinServerSec
Value Type: REG_DWORD - Number
Valid Range: same as NtlmMinClientSec
Default: 0
Description: This parameter specifies the minimum security to be used.
   0x00000010  Message integrity
   0x00000020  Message confidentiality
   0x00080000  NTLMv2 session security
   0x20000000  128 bit encryption
```

Checking domain information and VCS status

This appendix describes commands that can be used to check the status of the VCS's connection to the AD domain. In a clustered VCS system, each peer must be checked separately.

Domain_management

1. Login as root over SSH or via the serial interface.
2. Type:
   `domain_management`
   you will be presented with the options:
   `----------------------------------`
   `1) Join Domain`
   `2) Leave Domain`
   `3) VCS Status`
   `4) Domain Information`
   `5) Exit`
   `----------------------------------`
3. Choose option **`4) Domain Information`**.
   The VCS will report:

   ```
   LDAP server: <IP of AD server>
   LDAP server name: <AD server name>
   Realm: <AD DOMAIN (FQDN)>
   Bind Path: dc= .. dc= … (representing <DOMAIN>)
   LDAP port: <port, e.g. 389>
   Server time: <Time>
   KDC server: <IP of KDC server>
   Server time offset: <offset between AD server and VCS>

   Domain information request succeeded
   ```

4. Choose option **`3) VCS Status`**.
5. When asked, enter the domain administrator username.
6. When asked, enter the domain administrator password (case sensitive).
   The VCS will report:

   ```
   … <lots of details> …

   Domain status request succeeded
   ```

Note that the domain administrator username and password are not stored in VCS; they are only used in Join AD domain, Leave AD domain and VCS Status operations.

Net ads info

1. Login as root over SSH or via the serial interface.
2. Type:
   net ads info
   The VCS will report:

```
LDAP server: <IP of AD server>
LDAP server name: <AD server name>
Realm: <AD DOMAIN (FQDN)>
Bind Path: dc= .. dc= … (representing <DOMAIN>)
LDAP port: <port, e.g. 389>
Server time: <Time>
KDC server: <IP of KDC server>
Server time offset: <offset between AD server and VCS>

Domain information request succeeded
```

   This is the same information as option 4) of Domain_management.

Net ads testjoin

1. Login as root over SSH or via the serial interface.
2. Type:
   net ads testjoin
   The VCS will report:

```
[<Date, Time>] <success or failure logs>
Join to domain <success or failure>
```

   Failed reasons may include:
   Preauthentication failed
   To fix this, re-enter username and password on web interface and click **Save**.
   (You may have to edit another field on the web page to allow the username and password to be configurable – then return the field to the required value before clicking **Save**.)

Leaving a domain

Note: For clusters, a Leave Domain must be carried out for each peer.

To get VCS to leave the AD domain:

1. Login as root over SSH or via the serial interface.
2. Type:
   domain_management
   you will be presented with the options:

```
-----------------------------------
1) Join Domain
2) Leave Domain
3) VCS Status
4) Domain Information
```

```
5) Exit
-----------------------------------
```

3. Choose option **2 Leave Domain**.
4. When asked, enter the domain administrator username.
5. When asked, enter the domain administrator password (case sensitive).
   A successful Leave will result in the messages:

```
Deleted account for '<DNS Local hostname>' in realm '<AD DOMAIN (FQDN)>'
…
Domain leave succeeded
```

Note that the domain administrator username and password are not stored in VCS; they are only used in Join AD domain, Leave AD domain and VCS Status operations.

Example process for moving Jabber Video users to AD direct authentication

To migrate Jabber Video users to AD direct authentication:

1. Ensure that VCS is running version X6.1 or later code.
2. Upgrade all Jabber Video clients to version 4.2 or later.
   This can be achieved via provisioning – users will be alerted to the fact that a new version of code is available to download. See *Cisco Jabber Video for TelePresence Administrator Guide* for details.
3. Send out an email to all users requesting that they upgrade their Jabber Video.
   Explain that their login password will soon change to be their AD password, and that the **Username** in Jabber Video will need to be updated to "<AD Short Domain Name>\username".
   - The existing username must be the same as the AD username. If it is not, the authenticated name will not match the provisioning data username.
   - The username must not exceed 20 characters (due to a limitation in Active Directory).

   Explain that after a chosen date they will not be able to sign in to Jabber Video if they do not upgrade.
   Add a message for Jabber Video for Mac users: Mac-users will not get an upgrade prompt, they will have to download the new Jabber Video code and upgrade manually.
4. Configure the VCS for AD direct authentication, but set **NTLM protocol challenges** to *Off*.
5. When ready to switch over, on the VCS:
   a. Set up *Check Credentials* on the VCS Default Zone, and the Default Subzone (or relevant subzones).
   b. Set **NTLM protocol challenges** to *Auto*.
6. Send out a reminder email to users that their old Jabber Video and old password will no longer work, that they need to use Jabber Video 4.2 or later and their AD password and that the Jabber Video **Username** must be configured as "<AD Short Domain Name>\username".

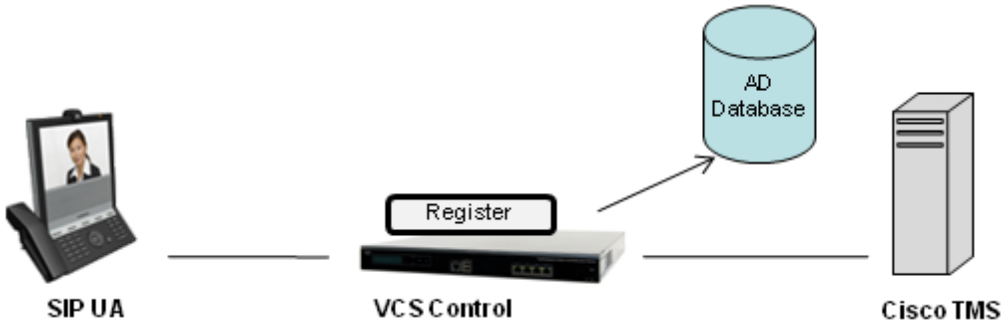
Example AD direct authentication deployments

When enabling authentication, there are a number of configuration architectures that may be considered.

- VCS Control with Active Directory (direct) authentication
- VCS Control and VCS Expressway, each with Active Directory (direct) authentication
- VCS Control and VCS Expressway with Active Directory (direct) authentication delegated to the VCS Control

VCS Control with Active Directory (direct) authentication

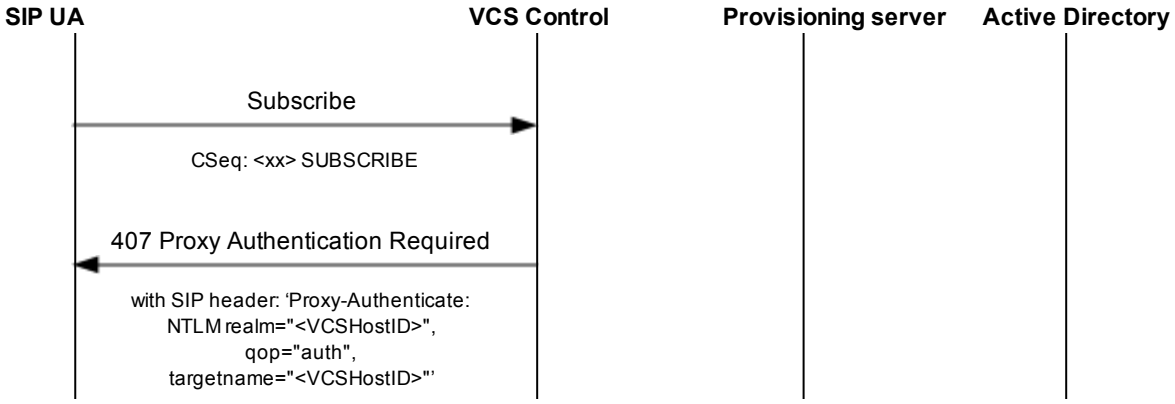
The SIP UA sends a request to the VCS Control and it challenges for authentication, sending the authentication details to the AD server for validation.

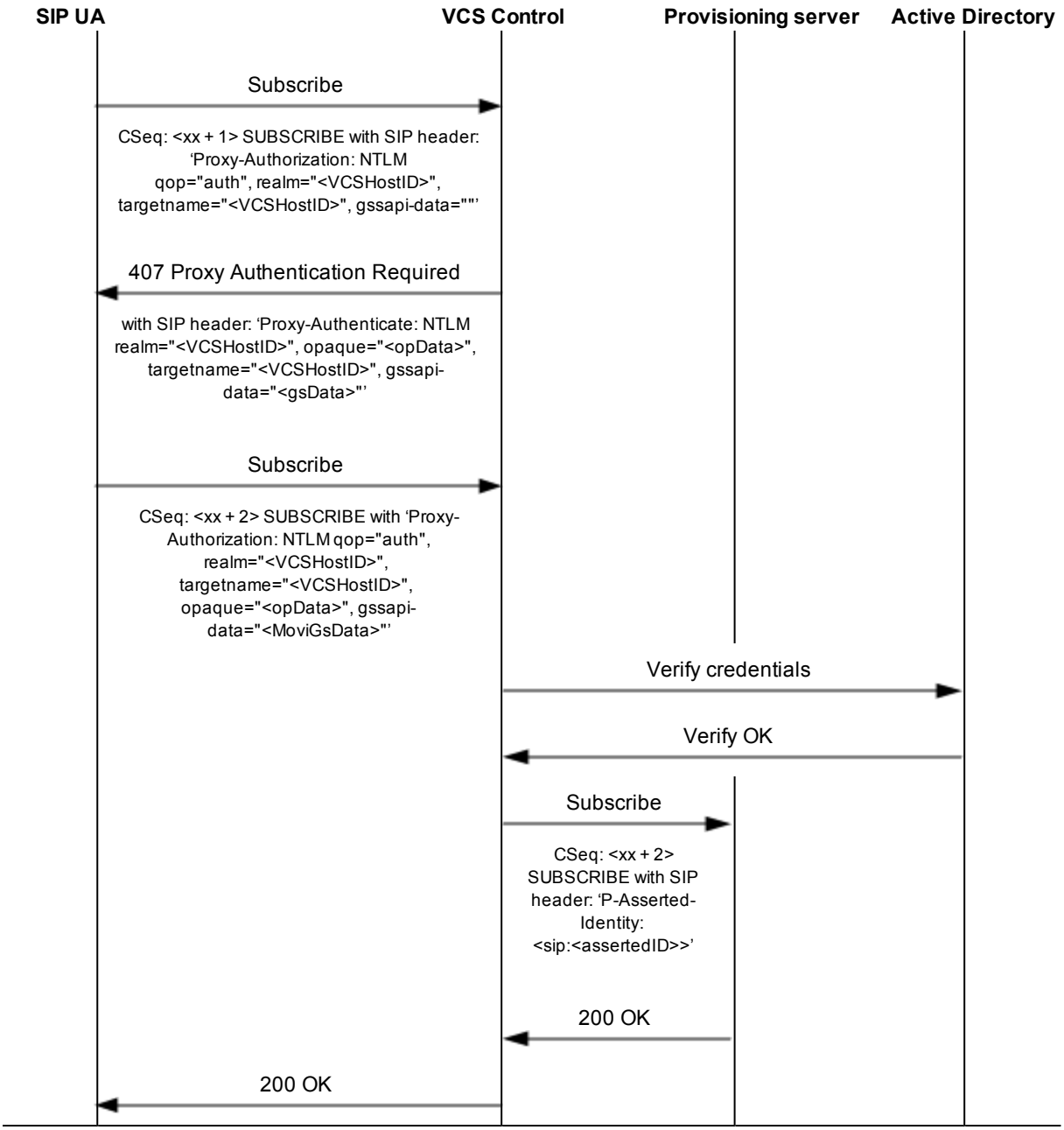


Setting	VCS Control
Provisioning	✓
AD configuration	✓
Default Zone	Check credentials
Default Subzone	Check credentials
SIP domain	Domain for SIP account

Setting	Cisco TMS
SIP Server	VCS Control IP address or FQDN

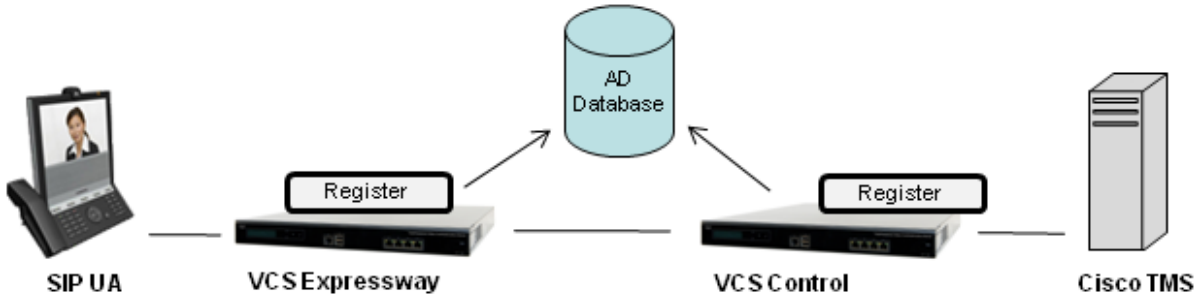
This example call flow diagram shows a subscribe for provisioning that is challenged using AD (direct) authentication:




SIP UA
VCS Control
Provisioning server
Active Directory
Subscribe
CSeq: <xx + 1> SUBSCRIBE with SIP header: 'Proxy-Authorization: NTLM qop="auth", realm="<VCSHostID>", targetname="<VCSHostID>", gssapi-data=""'
407 Proxy Authentication Required
with SIP header: 'Proxy-Authenticate: NTLM realm="<VCSHostID>", opaque="<opData>", targetname="<VCSHostID>", gssapi-data="<gsData>"'
Subscribe
CSeq: <xx + 2> SUBSCRIBE with 'Proxy-Authorization: NTLM qop="auth", realm="<VCSHostID>", targetname="<VCSHostID>", opaque="<opData>", gssapi-data="<MoviGsData>"'
Verify credentials
Verify OK
Subscribe
CSeq: <xx + 2> SUBSCRIBE with SIP header: 'P-Asserted-Identity: <sip:<assertedID>>'
200 OK
200 OK

VCS Control and VCS Expressway, each with Active Directory (direct) authentication

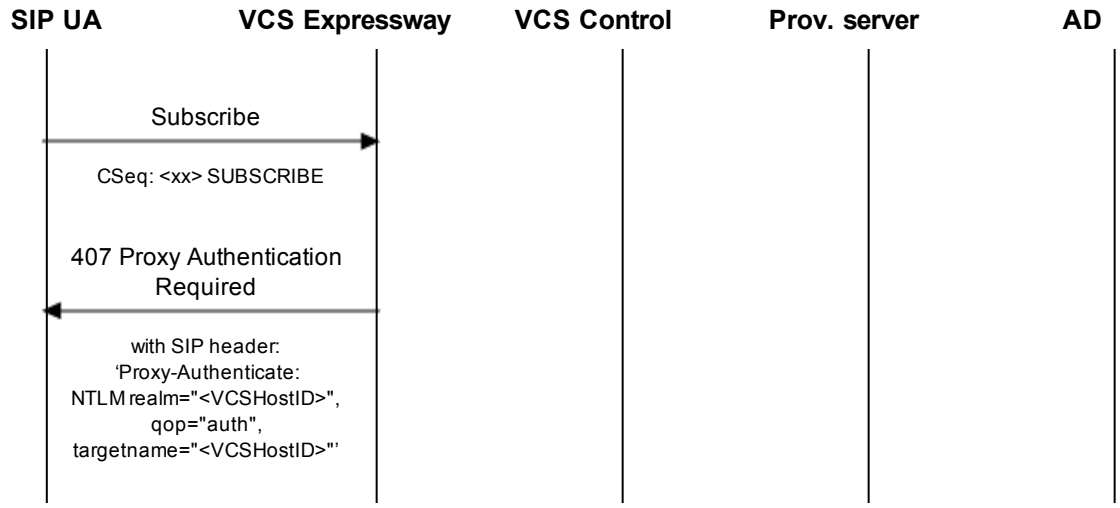
Both the VCS Expressway and the VCS Control can be configured to perform direct authentication against the AD server.

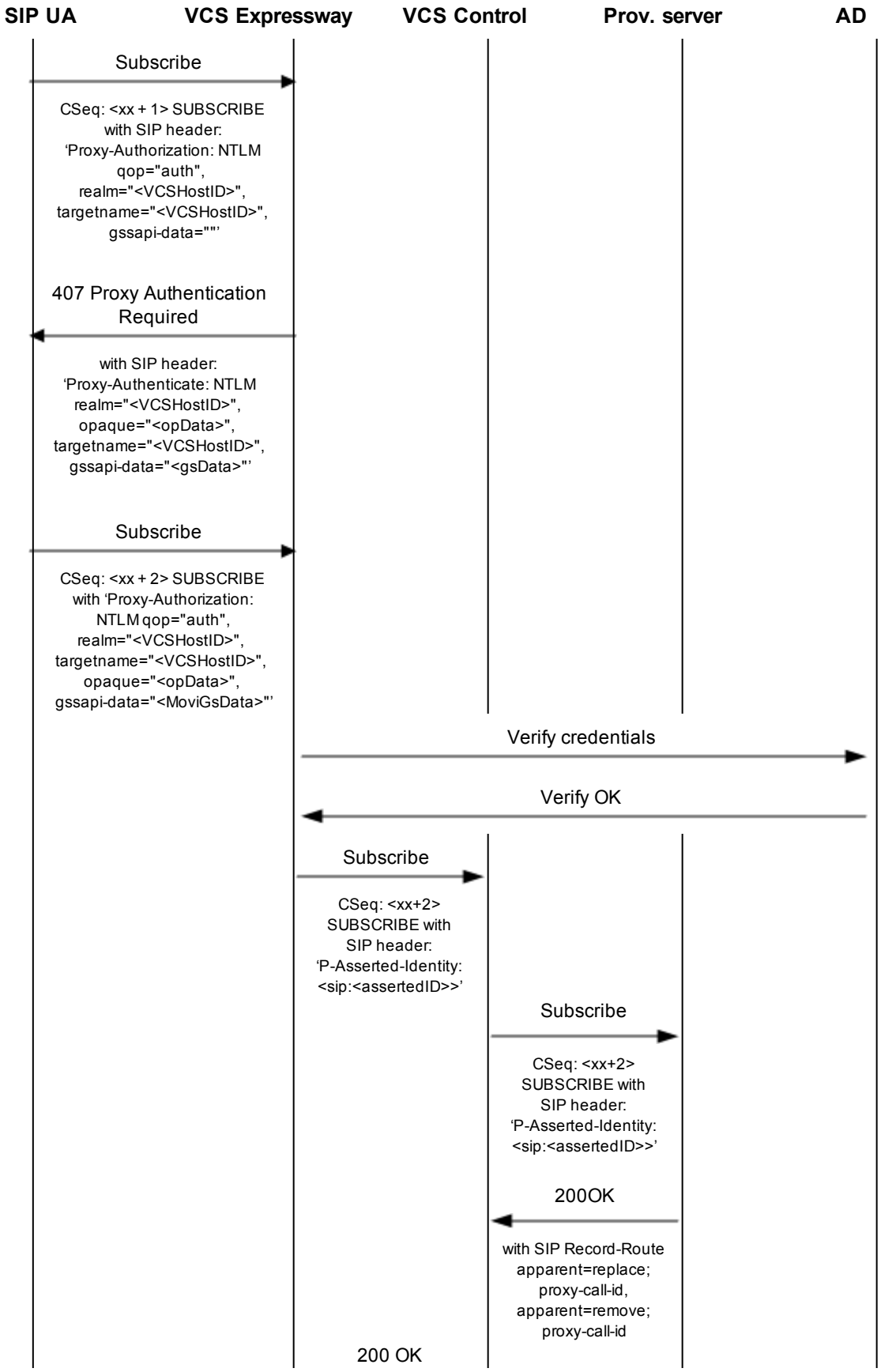


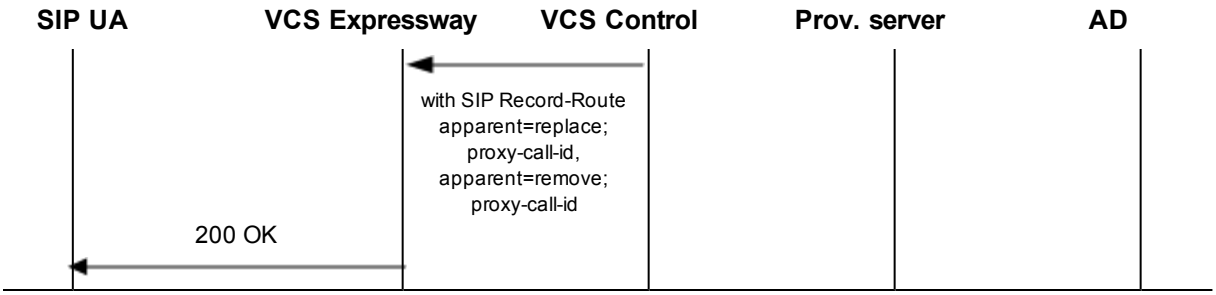
Setting	VCS Expressway	VCS Control
Provisioning	X	✓
AD configuration	✓	✓
Default Zone	Check credentials	Check credentials
Default Subzone	Check credentials	Check credentials
Traversal Zone	Check credentials	Check credentials
SIP domain	Domain for SIP account	Domain for SIP account
SIP registration proxy mode	Off	Off

Setting	Cisco TMS
SIP Server	VCS Control IP address or FQDN
Public SIP Server	VCS Expressway IP address or FQDN

This example shows a subscribe for provisioning that is challenged using an AD (direct) authentication challenge by the VCS Expressway. It is then forwarded on to the VCS Control which in turn passes it to the provisioning server:



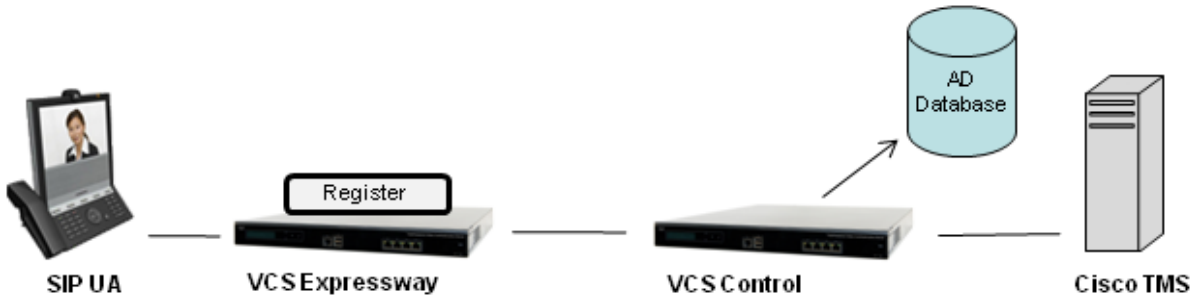

SIP UA
VCS Expressway
VCS Control
Prov. server
AD
Subscribe
CSeq: <xx + 1> SUBSCRIBE with SIP header: 'Proxy-Authorization: NTLM qop="auth", realm="<VCSHostID>", targetname="<VCSHostID>", gssapi-data=""'
407 Proxy Authentication Required
with SIP header: 'Proxy-Authenticate: NTLM realm="<VCSHostID>", opaque="<opData>", targetname="<VCSHostID>", gssapi-data="<gsData>"'
Subscribe
CSeq: <xx + 2> SUBSCRIBE with 'Proxy-Authorization: NTLM qop="auth", realm="<VCSHostID>", targetname="<VCSHostID>", opaque="<opData>", gssapi-data="<MoviGsData>"'
Verify credentials
Verify OK
Subscribe
CSeq: <xx+2> SUBSCRIBE with SIP header: 'P-Asserted-Identity: <sip:<assertedID>>'
Subscribe
CSeq: <xx+2> SUBSCRIBE with SIP header: 'P-Asserted-Identity: <sip:<assertedID>>'
200OK
with SIP Record-Route apparent=replace; proxy-call-id, apparent=remove; proxy-call-id
200 OK


SIP UA
VCS Expressway
VCS Control
Prov. server
AD
with SIP Record-Route
apparent=replace;
proxy-call-id,
apparent=remove;
proxy-call-id
200 OK

VCS Expressway with Active Directory (direct) authentication delegated to the VCS Control

If the VCS Expressway cannot be connected directly to the AD server, then authentication can be delegated to the VCS Control.

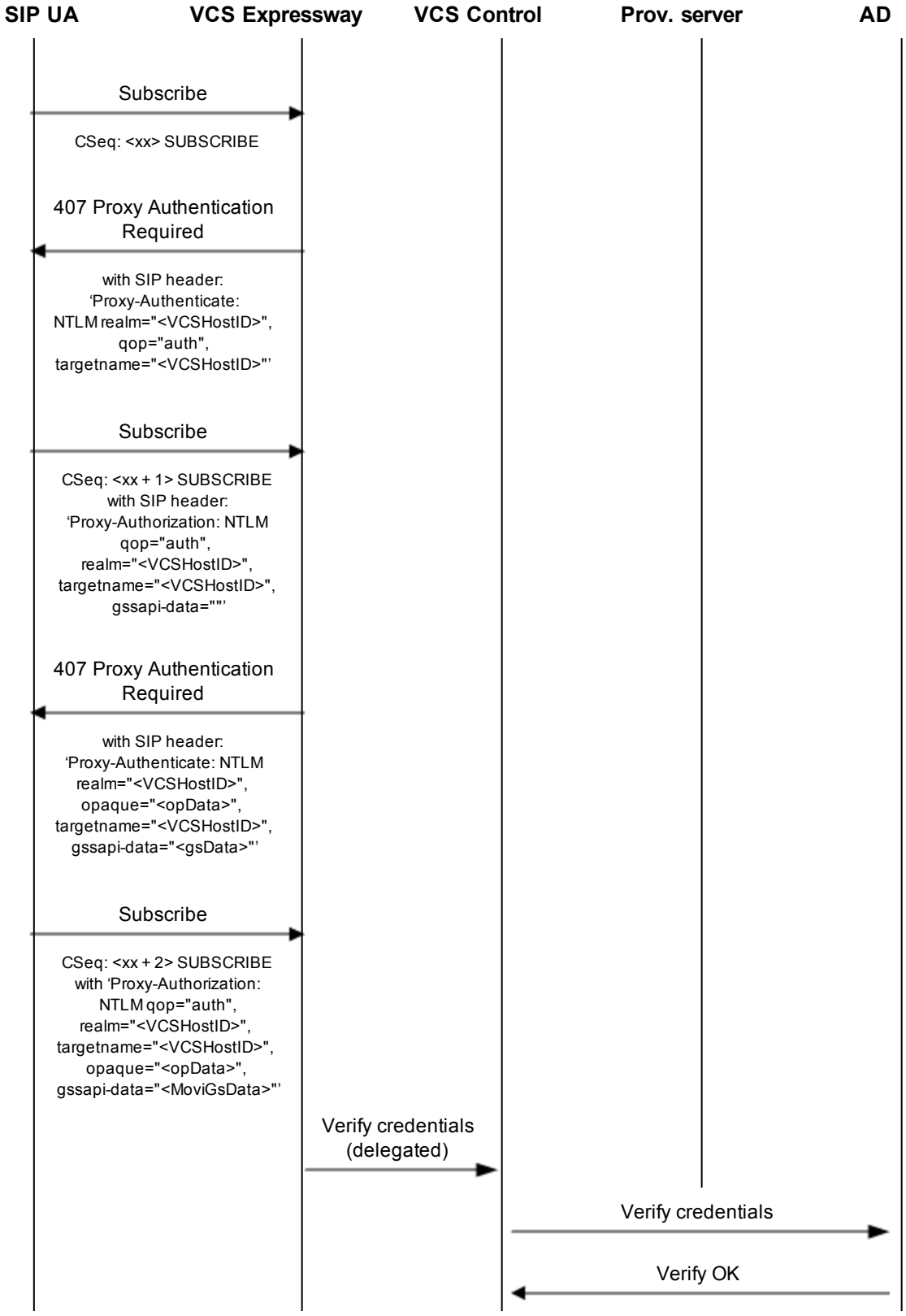
- The SIP UA sends a request to the VCS Expressway and the VCS Expressway challenges for authentication.
- The VCS Expressway delegates the checking of the SIP UA's credentials to the VCS Control, passing the authentication details to the VCS Control via the traversal zone.
- The VCS Control sends the authentication details to the AD server for validation and passes the result back to the VCS Expressway.
- The authenticated registration takes place on the VCS Expressway and does not have to be proxied to the VCS Control. This means media does not have to traverse the firewall in calls between SIP UAs that are both registered to the VCS Expressway.

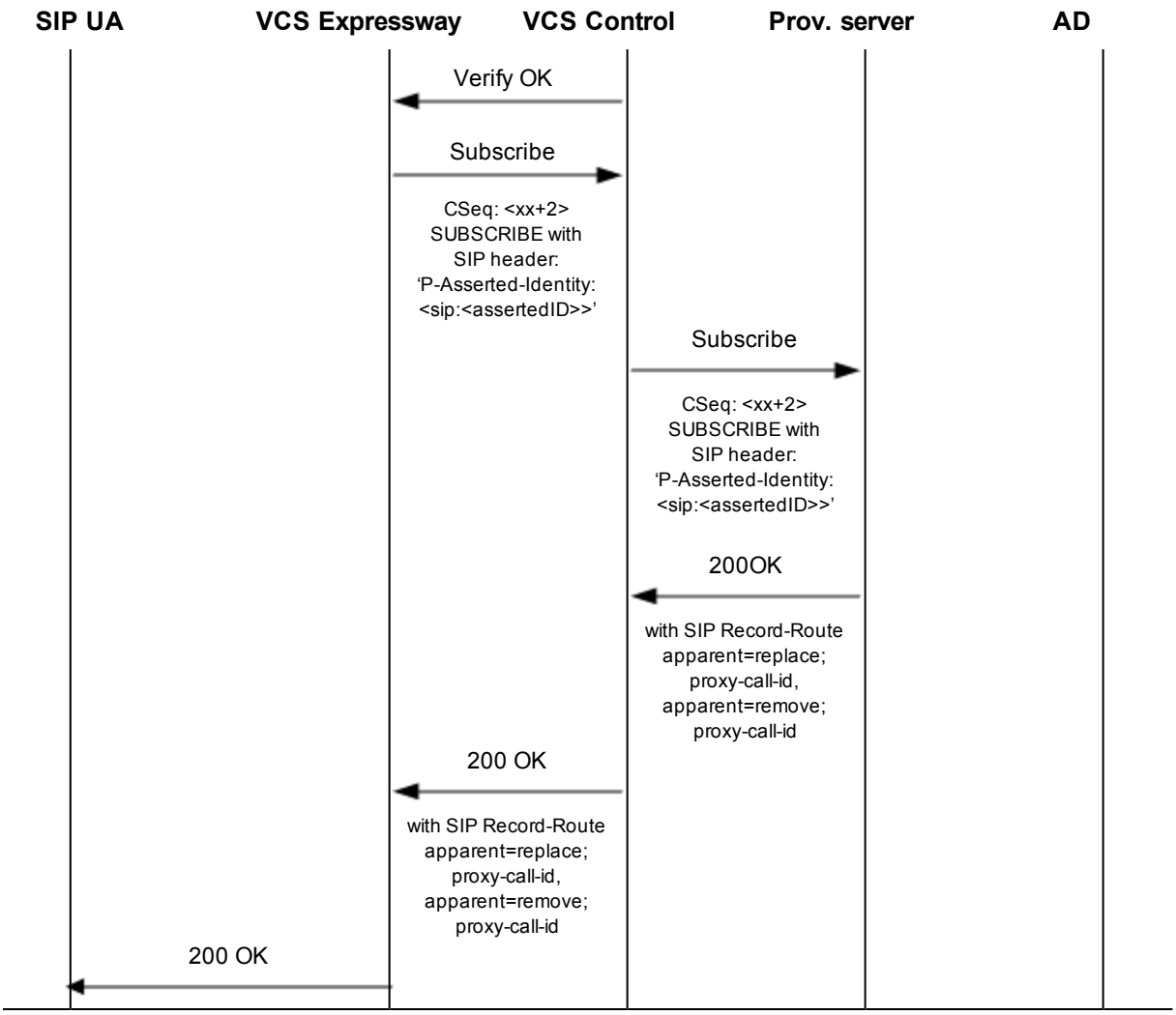


Setting	VCS Expressway	VCS Control
Provisioning	X	✓
AD configuration	X	✓
Default Zone	Check credentials	Check credentials
Default Subzone	Check credentials	Check credentials
Traversal Zone	Check credentials	Check credentials
SIP domain	Domain for SIP account	Domain for SIP account
SIP registration proxy mode	Off	Off
SIP delegated credential checking	On	On

Setting	Cisco TMS
SIP Server	VCS Control IP address or FQDN
Public SIP Server	VCS Expressway IP address or FQDN

This example shows a subscribe for provisioning that is challenged using an AD (direct) authentication challenge by the VCS Expressway. Credential checking is delegated to the VCS Control. The authenticated request is then forwarded on to the VCS Control which in turn passes it to the provisioning server:




SIP UA
VCS Expressway
VCS Control
Prov. server
AD
Verify OK
Subscribe
CSeq: <xx+2>
SUBSCRIBE with
SIP header:
'P-Asserted-Identity:
<sip:<assertedID>>'
Subscribe
CSeq: <xx+2>
SUBSCRIBE with
SIP header:
'P-Asserted-Identity:
<sip:<assertedID>>'
200OK
with SIP Record-Route
apparent=replace;
proxy-call-id,
apparent=remove;
proxy-call-id
200 OK
with SIP Record-Route
apparent=replace;
proxy-call-id,
apparent=remove;
proxy-call-id
200 OK

Document revision history

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

Revision	Date	Description
8	June 2014	Republished for X8.2.
7	December 2013	Updated for VCS X8.1, including delegated credential checking.
6	August 2012	Updated for VCS X7.2.
5	March 2012	Updated for VCS X7.1, including use of Cisco TMS Provisioning Extension mode.
4	February 2012	Added additional overview information on configuring authentication policy.
3	November 2011	Additional information on checking and setting NTLM versions on Movi PC.
2	August 2011	Updated for VCS X7.0.
1	May 2011	Initial release.