Device authentication on Cisco VCS

Deployment Guide

Cisco VCS X7.2

D14819.06

August 2012

Contents

Introduction

Device authentication is the verification of the credentials of an incoming request to the Cisco TelePresence Video Communication Server (Cisco 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 will be 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 its authentication policy, and then accept or reject the message accordingly.

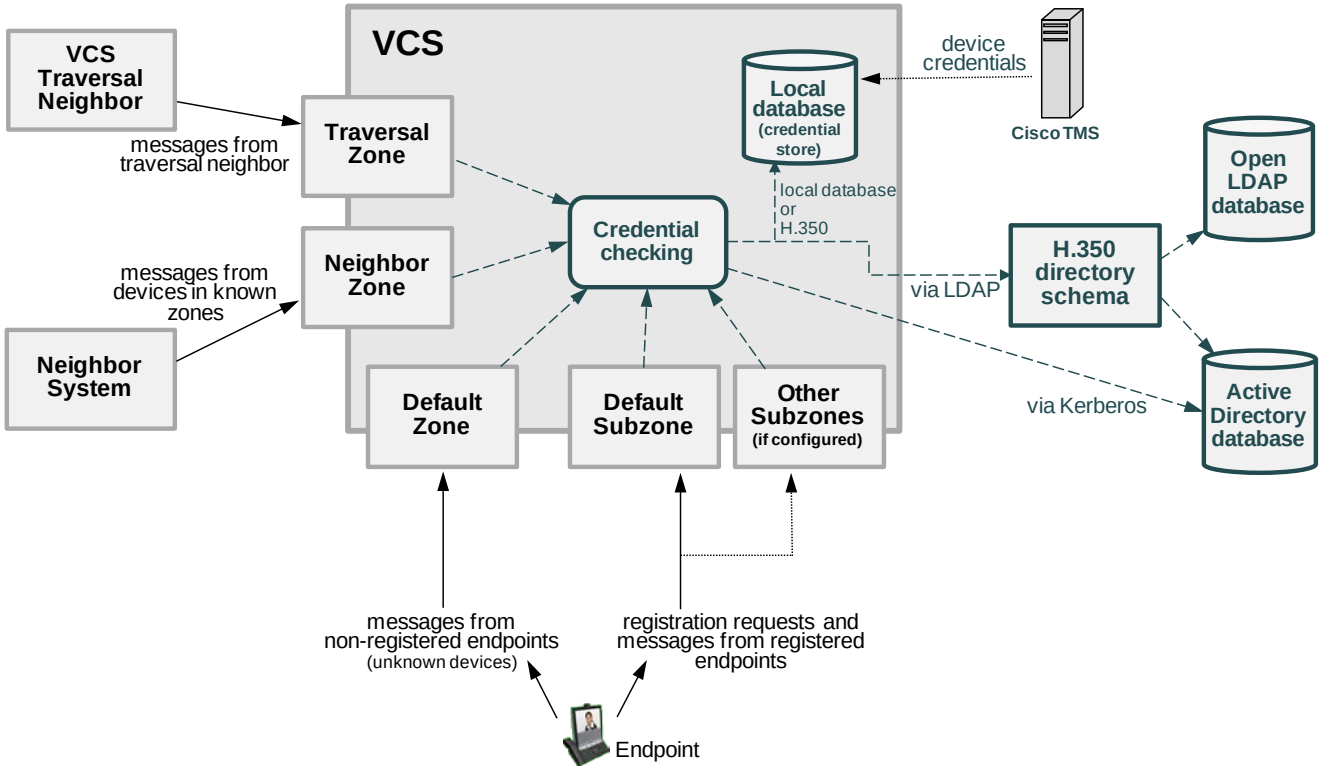
VCS authentication policy can be configured separately for each zone and subzone. This means that both authenticated and unauthenticated devices could be allowed to register to, and communicate with, the same VCS if required. Subsequent call routing decisions can then be configured with different rules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

As from version X7.2, 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. See Configuring VCS authentication methods for more information.

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



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, phonebooks and calls) from that zone or subzone and whether those messages are rejected, treated as authenticated, or treated as unauthenticated within the VCS.

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.

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 phonebook 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. A full description of the various authentication policy behaviors is contained in the *VCS Administrator Guide* (and is also available in the VCS online help).

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 the **Edit zone** page (**VCS 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 the **Edit subzone** page (**VCS 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.

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 Cisco 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.

Device provisioning and authentication policy

VCS X7.1 and X7.2 supports two provisioning modes:

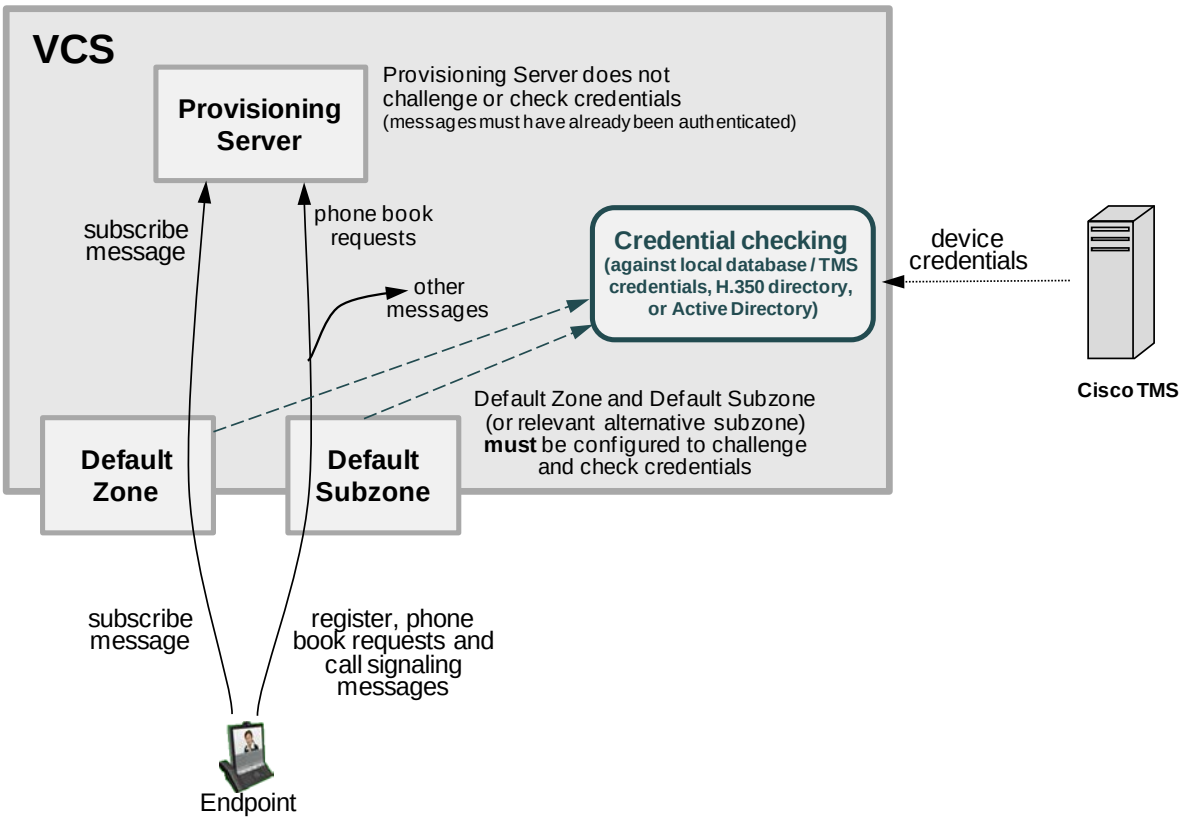
- TMS Provisioning Extension mode
- TMS Agent legacy mode

The Provisioning Server (hosted on the VCS) has different device authentication requirements depending on the provisioning mode.

TMS Provisioning Extension mode

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 TMS.

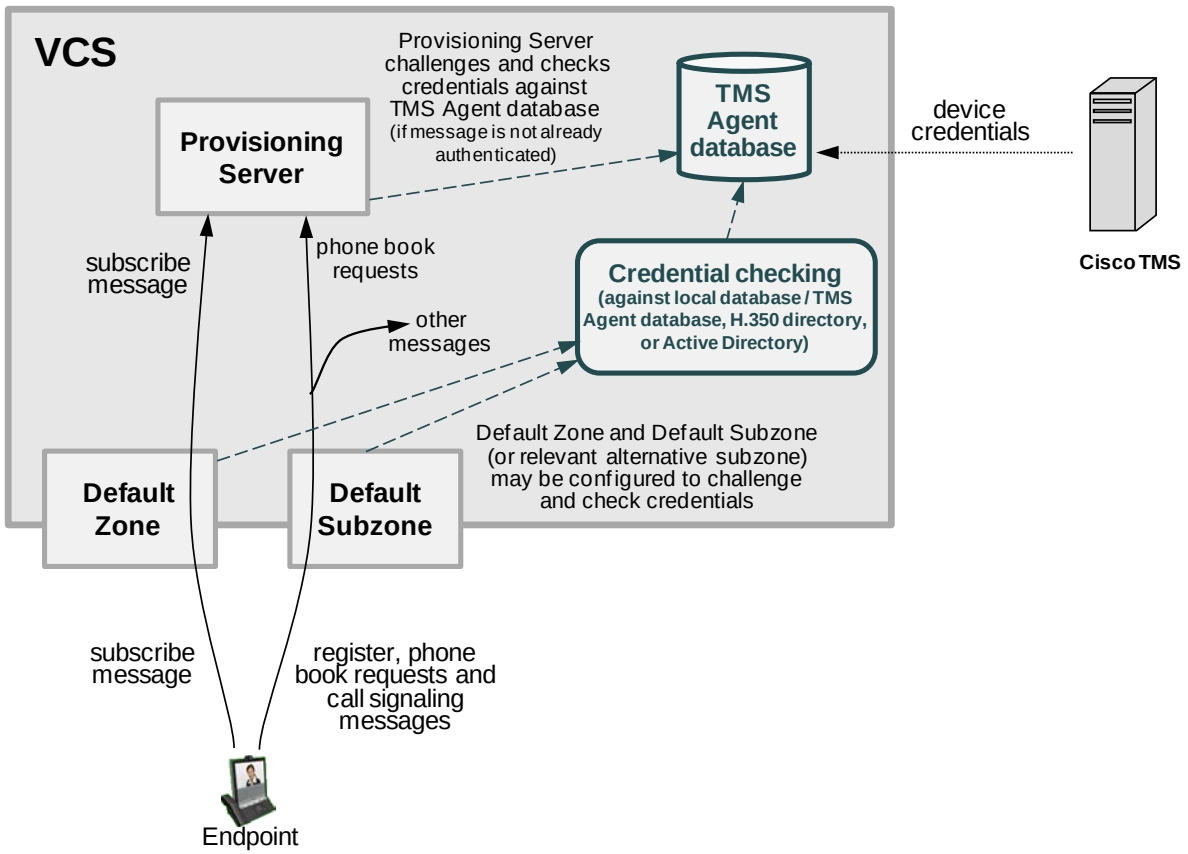
For more information about provisioning configuration in general, see *Cisco TMS Provisioning Extension Deployment Guide*.

Legacy TMS Agent mode

The Provisioning Server will only service authenticated provisioning requests, but it can perform its own authentication challenge:

- If the VCS has already authenticated the device (at the zone or subzone entry point), then the Provisioning Server accepts the VCS's authentication check and does not perform any additional authentication challenge.
- If the VCS has not authenticated the device, then the Provisioning Server will authenticate the request (i.e. challenge for and check credentials) before providing provisioning data.
  - The Provisioning Server checks device account credentials against the TMS Agent database only. It does not check against any other credential store.

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



Note that:

- 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).
- Subsequent messages, including registration requests, phone book requests and call signaling messages go through the Default Subzone (or relevant alternate subzone).

Cisco VCS Starter Pack Express

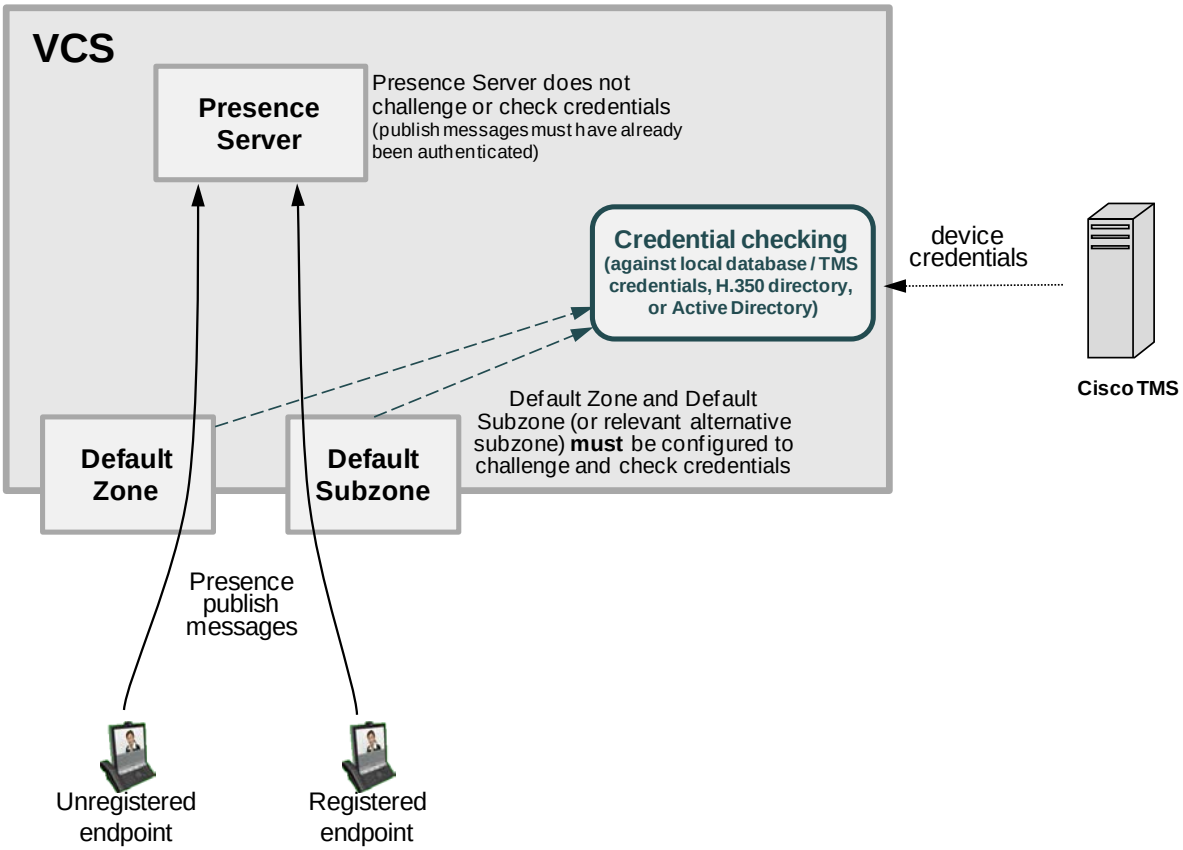
The Provisioning Server on a Cisco VCS Starter Pack Express operates in the same manner as for TMS Provisioning Extension mode – it does not challenge provisioning requests. It provisions devices only if the request has already been authenticated by the VCS (at the zone or subzone entry point).

Presence and authentication policy

The Presence Server on VCS 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 TMS (in either TMS Agent legacy mode or TMS Provisioning Extension mode).

Hierarchical dial plan (directory VCS) deployments

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 TMS Provisioning Extension mode), 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 the **Zones** page (**VCS 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 non-traversal and traversal licenses on each directory VCS to handle those calls going between each subnetwork.

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*.

Practical configuration of authentication policy

VCS Control

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

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, it is recommended 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 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.

Use registration allow and deny lists to limit what can register to the 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.

See also Appendix 12 — Example AD direct authentication deployments.

Configuring VCS authentication methods

The VCS supports 3 different methods of verifying authentication credentials:

- against an on-box local database (which includes any 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)

As from version X7.2, 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.

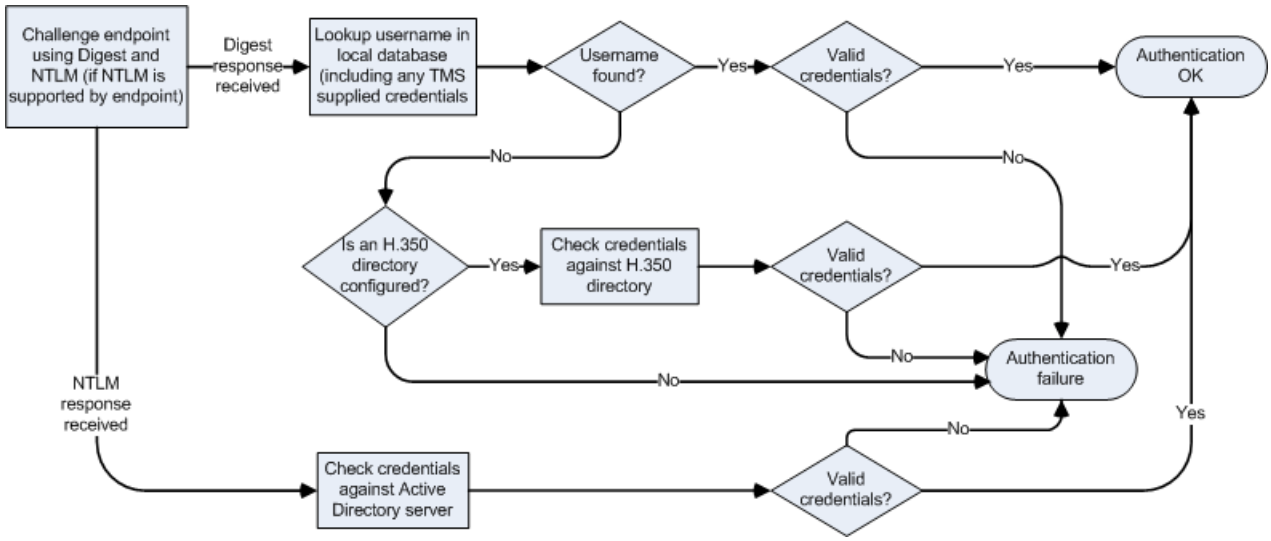
(Prior to version X7.2, the VCS could be configured to verify credentials against either the local database or an H.350 directory service.)

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, Movi / Jabber Video 4.2 or later only. 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 it authenticates the credentials supplied by an endpoint.



Using 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

The local database credentials are configured on the **Local authentication database** page. To enter a set of device credentials:

1. Go to **VCS 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 endpoint - you do not need to have a separate entry in the database for each endpoint.

Credentials managed within TMS (for device provisioning)

The local database includes any credentials supplied by TMS, in addition to any entries that have been added manually.

Incorporating TMS credentials within the local database aids migration from a provisioning-only authenticated system to a configuration where all messages are authenticated – it means that VCS can authenticate all messages against the credentials generated by TMS which were previously used by the Provisioning Server just to authenticate provisioning requests (i.e. no change of password is required for provisioned devices).

TMS Agent legacy mode

The credentials supplied by the TMS Agent are stored in a separate TMS Agent database. The VCS checks credentials by looking in both the local authentication database and the TMS Agent database.

(Prior to X7.0, the VCS did not check against the TMS Agent database, it only checked the manually configured credentials in the local database.)

TMS Provisioning Extension mode

When the VCS is using the 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.

Using the local database with other authentication mechanisms

Local database authentication in combination with H.350 directory authentication

From version X7.2, you can configure the VCS to use both the local database and a H.350 directory.

- If a 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.

(Prior to version X7.2, the VCS could be configured to verify credentials against either the local database or an H.350 directory service.)

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

An H.350 directory service lookup can be used for authenticating any endpoint, SIP and H.323.

Configuring the VCS to use an H.350 directory service lookup

Install the H.350 schemas on the LDAP server:

1. Download the required H.350 schemas from the VCS and install them on the LDAP server.

   See the *VCS Administrator Guide* or VCS online help for instructions about how to download the schemas and for how to configure a Microsoft Active Directory LDAP server or an OpenLDAP server.

To enable and configure access to an LDAP server for H.350 directory service lookup:

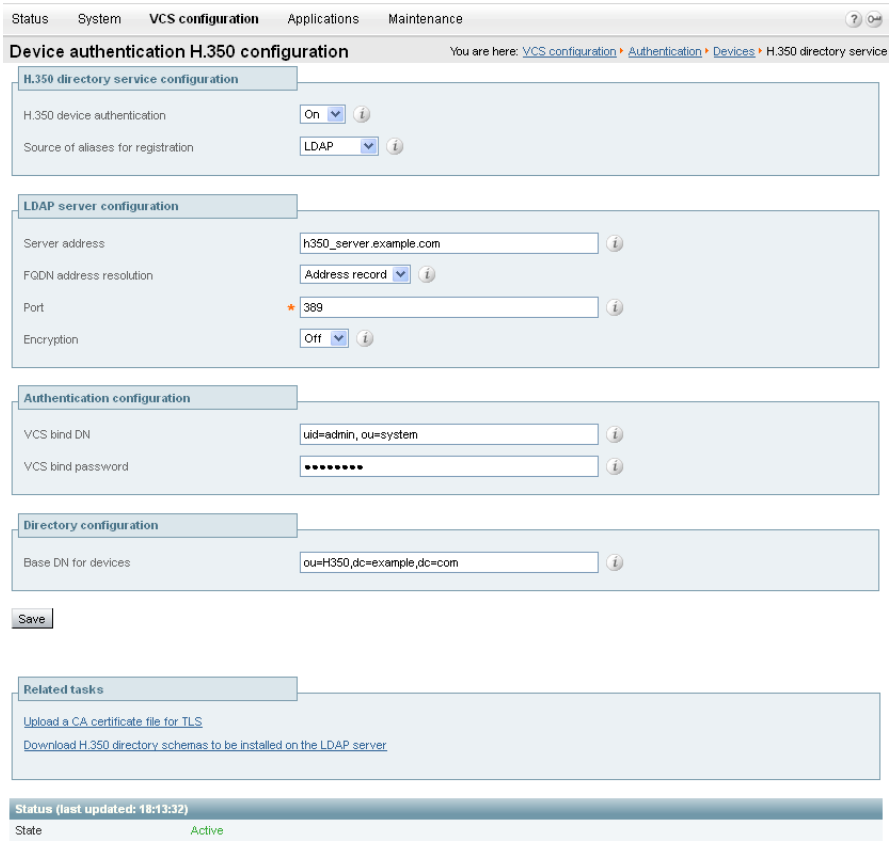
1. Go to **VCS configuration > Authentication > Devices > H.350 directory service**.
2. Configure the fields as follows:

H.350 device authentication	Select *On*.
Source of aliases for registration	This determines how aliases are checked and registered after the endpoint has had its authentication credentials verified. The options are: *H.350 directory*: the aliases presented by the endpoint are checked against those listed in the H.350 directory. *Endpoint*: only the aliases presented by the endpoint are used. *Combined*: the aliases presented by the endpoint are used in addition to any listed in the H.350 directory. The default value is *H.350 directory*.
LDAP server address	Enter the IP address or fully-qualified domain name (FQDN) 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.
Port	Typically 389 for non secure connections and 636 for secure connections.
Encryption	*Off* or *TLS* Note that if encryption is set to TLS, a valid CA certificate, private key and server certificate must be uploaded to the VCS via the **Trusted CA certificate** and **Security certificate** pages (located under **Maintenance > Certificate management**). The default value is *Off*.
VCS bind DN	Distinguished name of username used when binding to the H.350 LDAP server (for example, uid=admin, ou=system).
VCS bind password	Password to use when binding to the H.350 LDAP server.
Base DN for devices	Distinguished name to use when connecting to the H.350 LDAP server (for example, ou=H350,dc=example,dc=com).

3. Click **Save**.

Connection is successful when the Status reports State Active.

Note that authentication credentials (for Digest challenges) are always checked first against the local database. The H.350 directory service is subsequently checked only if the username is not found in the local database.



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.

- 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.

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.

- Active Directory database (direct) authentication 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.
  - In such circumstances you could, for example, use the Active Directory (direct) server method for Movi / Jabber Video, and the local database or H.350 directory service authentication for the other devices that do not support NTLM.
- NTLM authentication is only supported (at the time of writing) by Movi / Jabber Video version 4.2 or later

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.

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 Cisco 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.)

Cisco VCS

- The VCS must be configured to use a DNS server (**System > DNS**).
  - The VCS’s **Local 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 Cisco VCS peer has a unique **Local host name**.
- Ensure that an NTP server (**System > Time**) has been configured and is active.
- Ensure that the VCS is configured to challenge for authentication on the relevant zones and subzones:
  - The Default Zone (**VCS 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 (**VCS 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.

Note that setting up your VCS's authentication policy to check credentials will affect all devices (not just Movi) that send provisioning, registration, presence, phone book and call requests to the VCS.

Endpoint

- The PC on which Movi runs must use appropriate settings which match the settings of the AD server (see Appendix 4 — Active Directory (direct): Movi PC and AD server compatibility configuration).

IT request

You can use the questionnaire in Appendix 1 — IT requisition to get the appropriate information from your IT department).

Configure Active Directory server details in Cisco VCS

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

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

Connect to Active Directory Service	*On*
NTLM protocol challenges	Controls whether or not the VCS sends NTLM protocol challenges (in addition to Digest challenges) when authenticating devices over SIP. ■ Under normal operation this should be set to *Auto* where the VCS decides, based on the device type, whether to send NTLM challenges. ■ If you are migrating from an existing authentication mechanism to Active Directory (direct) 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).
AD domain	<AD DOMAIN> This must be the qualified domain name (QDN) of the AD domain and must be entered in CAPITALS. For example, EXAMPLE.COM.
Short domain name	<AD Short Domain Name> (this is also known as the NetBIOS Domain Name). For example, EXAMPLE.
Secure channel mode	*Auto* / *Enabled* / *Disabled* This configures the authentication used on the communications between VCS and the AD Domain Controller. Generally this should be left at its default value *Auto*.
Encryption	*Off* / *TLS* This configures whether TLS encryption is used between VCS and the Active Directory server. Note that if encryption is set to TLS, a valid CA certificate, private key and server certificate must be uploaded to the VCS via the **Security certificates** page (**Maintenance > Certificate management > Security certificates**). The default value is *TLS*.
Clockskew (seconds)	<Skew value in seconds> This sets up the maximum clock skew allowed between the VCS and the KDC

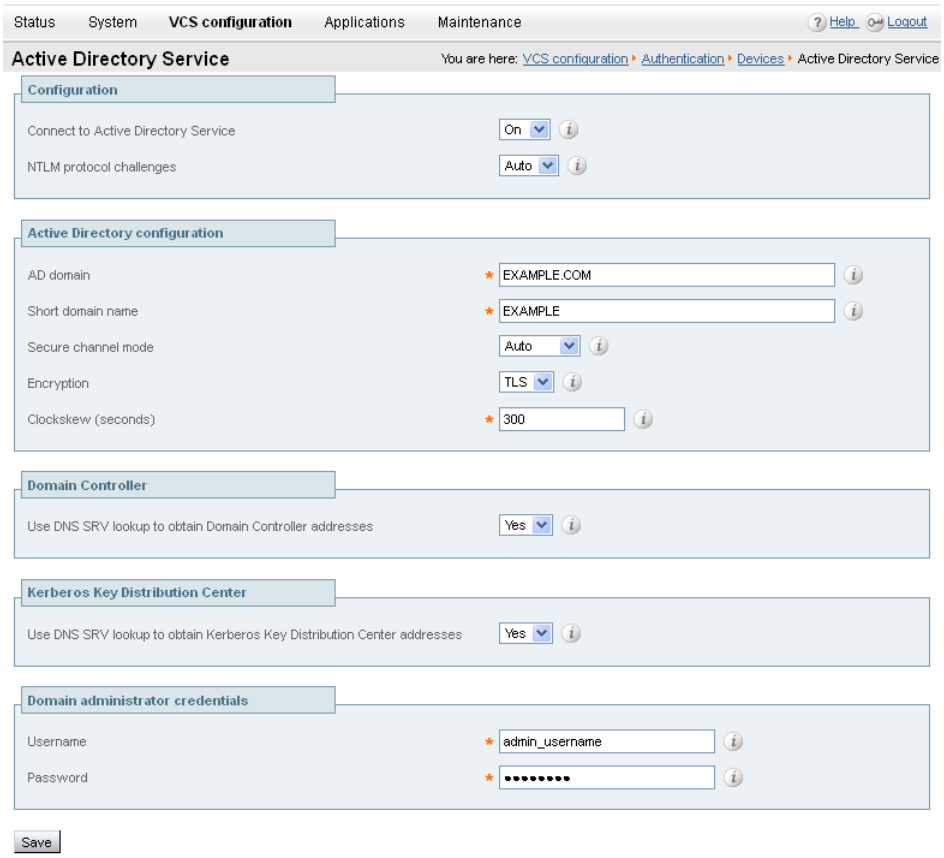
	(Kerberos Key Distribution Center). It should be kept in step with the clock skew setting on the KDC; generally this will be its default value of 300 (5 minutes). Ensure that VCS and KDC are synchronized to time servers.
Use DNS SRV lookup to obtain Domain Controller addresses	You are recommended to leave this field set to *Yes*. This means that VCS will use a DNS SRV lookup of <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	You are recommended to leave this field set to *Yes*. This means that VCS will use a DNS SRV lookup of <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. Note that Key Distribution Center addresses are typically the same as the Domain Controller addresses.
Username and **Password**	Enter the AD domain administrator username and password. The password is case sensitive. The credentials must be supplied whenever 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

   You can also check 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.



- 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 – see Appendix 8 — Active Directory (direct): Leaving 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.

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.

   Ensure that the master peer has successfully joined the AD domain before continuing.

On each other peer in turn:

2. Go to **VCS configuration > Authentication > Devices > Active Directory Service**.
3. Check that the configuration entered on the master peer has been replicated to the current peer.
4. Enter the AD domain administrator **Username** and **Password**.
   (These credentials are not stored by the VCS and so have to be entered each time.)
5. 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)

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

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

1. Go to **VCS 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.

Enable 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 Movi / Jabber Video (4.2 or later) with NTLM authentication challenges.

1. Go to **VCS 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.

Configure Movi / Jabber Video and test Active Directory database (direct) authentication

You are recommended to use a Movi configuration that already authenticates successfully using either provisioning or VCS authentication. This means that Movi's Advanced settings (**Internal VCS**, **External VCS** and **SIP domain** entries) are correctly configured.

1. Sign in to Movi:
   a. In the **Username** field, configure <AD Short Domain Name>\username (this field is not case sensitive).
   b. In the **Password** field, enter the password as configured in the Active Directory database for the chosen user.
2. Click **Sign in**.

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

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.

401 unauthorized returned from the provisioning server to a SUBSCRIBE for provisioning

If a “401 unauthorized” is returned from the TMS Agent provisioning server after the VCS has sent a SUBSCRIBE to it with a P-Asserted-Identity header, check that provisioning has been configured for this user.

For details on configuring provisioning, see the *Cisco TMS Provisioning Deployment Guide* (document D14368) and the *Cisco TMS Provisioning Troubleshooting Guide* (document D14427).

Movi / Jabber Video fails to authenticate

Mismatch of NTLM versions

In order to use Active Directory (direct) mode, the PC running Movi must use appropriate settings which are compatible with the AD server. To check (and change if required), see “Appendix 4 — Active Directory (direct): Movi PC configuration”.

Username too long

The Movi 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)

Log Code	Description
0xC000006C	Password policy not met
0xC000006D	The attempted logon is invalid due to a bad user name
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 (TMS PE 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 Movi 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 Movi sign in username all match (note that from X7.1 and later, usernames are case insensitive).
  - If the Movi sign in username and the authentication credential name do not match then the initial Subscribe will be rejected as unauthorized.
  - If the Movi 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

Movi 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 — 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 Cisco 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 Cisco VCS can be configured to access the Active Directory server to authenticate video endpoint calls.

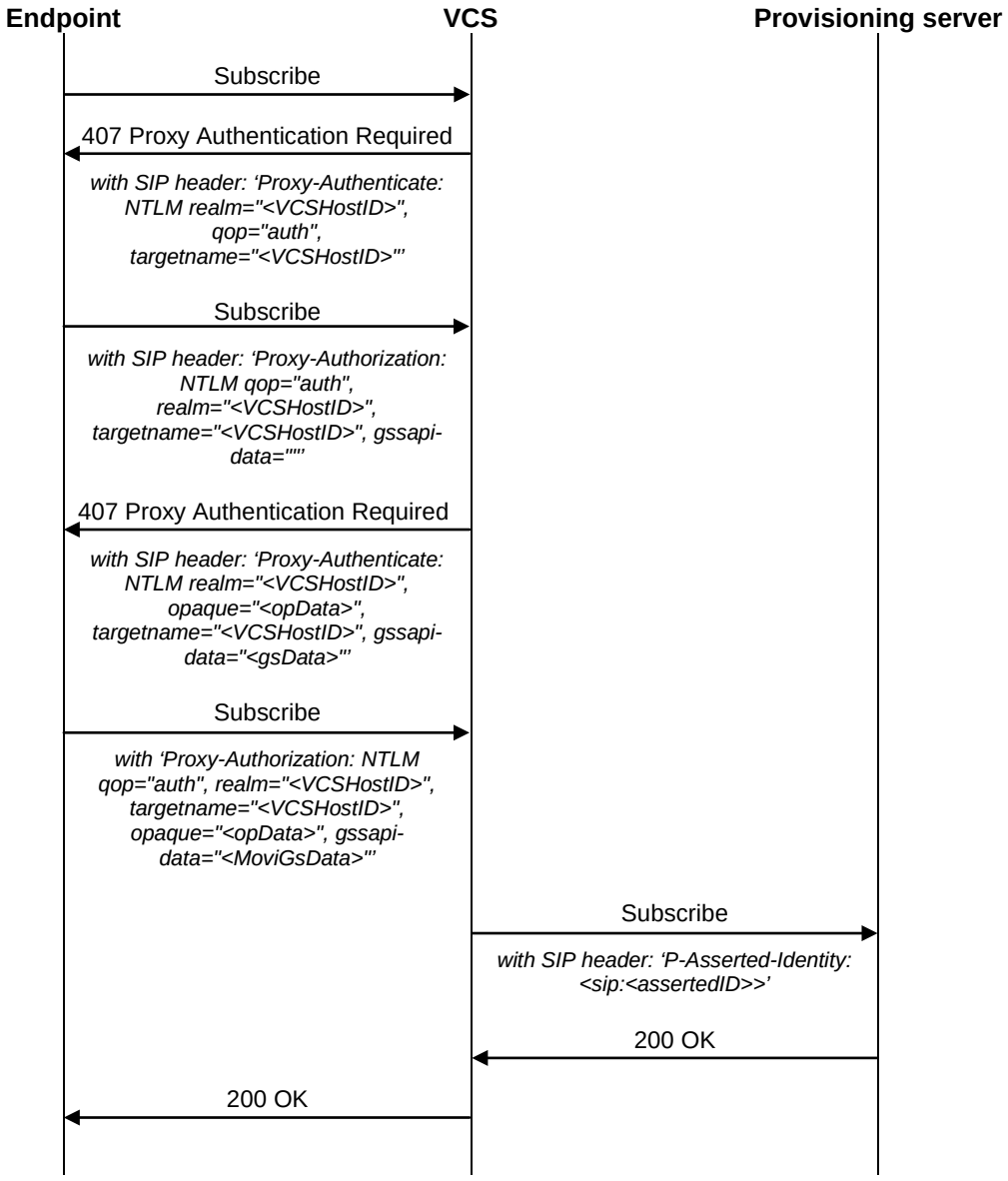
Active Directory Domain (FQDN)	
Active Directory Short Domain Name (NetBIOS Domain Name)	
Is a secure channel required between VCS and the AD domain controller?	YES / NO
Is TLS encryption needed between VCS and the AD server? Certificate location?	YES / NO Path to certificate file:
Is a clock skew value 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 — SIP messages for a provisioning subscription

Active Directory (direct)

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.



Appendix 4 — Active Directory (direct): Example DNS SRV configuration for AD

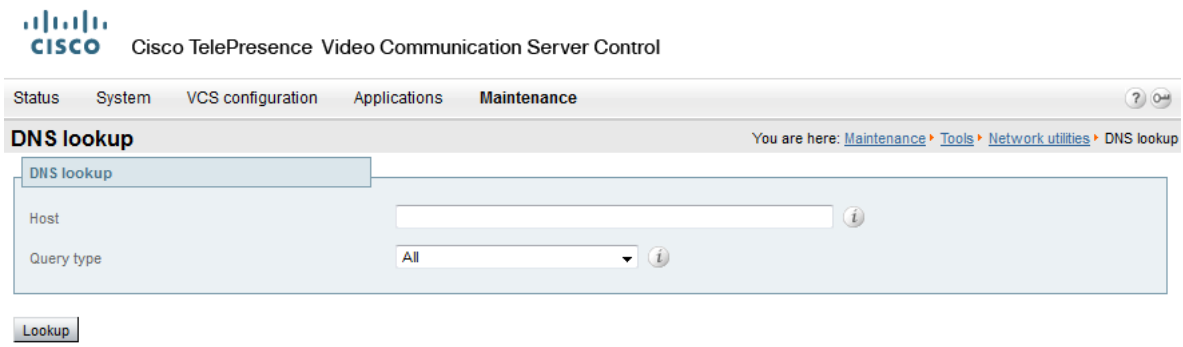
DNS SRV values needed

The following is a list of DNS SRV records that VCS will expect to find. DNS SRV records will be set up automatically by the AD server if the AD server 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.

Web browser checking of DNS SRV settings

Go to **Maintenance > Tools > Network utilities > DNS lookup**.



Enter the SRV path in the Host field and click **Lookup**.

Dig command to check DNS SRV settings

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:

```
; <lt;>> DiG 9.2.2 <lt;>> <DNS server> -t any <full dnssrv record>
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3072
;; 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 0 100 389 <A record 2>.

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

;; Query time: 0 msec
;; SERVER: <DNS server>#53(10.1.1.16)
;; WHEN: Wed Oct  7 14:39:31 2004
;; MSG SIZE  rcvd: 171
```

Appendix 5 — Active Directory (direct): Movi PC and AD server compatibility configuration

LMCompatibility level for Movi and the AD server

LMCompatibility level is set both on clients (e.g. Movi PC) and the Domain Controller hosting the Active Directory server. It is important that the values selected on the Movi 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:

Movi client PC

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

AD Domain Controller

Level	DC accepts		
	LM	NTLM	NTLM 2
0	✓	✓	✓
1	✓	✓	✓
2	✓	✓	✓
3	✓	✓	✓
4	-	✓	✓
5	-	-	✓

Compatibilities

AD Domain Controller Level	Movi 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**" Movi 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 Movi 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
```

Appendix 6 — IP Ports used on VCS for authentication

H.350 directory service

The following table lists the ports used for device authentication between VCS and the H.350 directory service server:

VCS port	Destination port	Usage
TCP/40000 .. 49999	TCP/389 or TCP/636	H.350 LDAP server

Active Directory (direct)

The following table lists the ports used for device authentication between VCS and the AD system:

VCS port	Destination port	Usage
UDP/10000 .. 10210	UDP/53	DNS Server
UDP/40000 .. 49999	UDP/88	Kerberos Key Distribution Center
TCP/40000 .. 49999	TCP/88	Kerberos
UDP/40000 .. 49999	UDP/389	VCS with Domain Controller
TCP/40000 .. 49999	TCP/389 or TCP/636	VCS with Domain Controller
TCP/40000 .. 49999	TCP/445 or TCP/139	Client credential authentication with the Domain Controller. VCS initially tries port 445, but if that cannot be reached tries port 139.

Appendix 7 — Active Directory (direct): 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, then type:

   ```
   domain_management
   ```

   you will be presented with the options:

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

2. 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
   ```

3. Choose option `3) VCS Status`
4. When asked, enter the domain administrator username
5. When asked, enter the domain administrator password (case sensitive)

   (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.)

   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, then 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>
```

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, then 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 select **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 selecting **Save**.)

Appendix 8 — Active Directory (direct): Leaving a domain

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

To get VCS to leave the AD domain, access to VCS via the root login is required.

1. Login as root over SSH or via the serial interface, then type:
   a. domain_management
      you will be presented with the options:

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

   b. Choose option 2 Leave Domain
   c. When asked, enter the domain administrator username
   d. When asked, enter the domain administrator password (case sensitive)

Note: 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.

- A successful Leave will result in the messages:
  Deleted account for '<DNS Local hostname>' in realm '<AD DOMAIN (FQDN)>'
  …
  Domain leave succeeded

Appendix 9 — Certificates for TLS

For the Cisco VCS to connect to a server over TLS, it must have a root CA certificate loaded that authorizes that server's server certificate.

In large organizations the IT department will be able to provide relevant certificate information. Details on how to process the supplied certificate, and how to create the root CA certificate are described in *Certificate Creation and Use with VCS Deployment Guide*.

If a root CA certificate is already loaded that is required for other purposes, this new root CA certificate should be concatenated with the other root CA certificate (Trusted CA certificate) and the single file containing the two certificates uploaded to Cisco VCS.

Appendix 10 — Use with Cisco VCS clusters

Active Directory (direct)

All authentication configuration is replicated across cluster peers, however the DNS server is configurable independently on each Cisco 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.

Appendix 11 — Example process for moving Movi / Jabber Video users to AD direct authentication

1. Ensure that Cisco VCS is running version X6.1 or later code.
   Follow the release notes or relevant cluster deployment guide to do the upgrade.
2. Upgrade all Movi / 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 *Movi / Jabber Video Administrator Guide* for details.
3. Send out an email to all users requesting that they upgrade their Movi.

   Explain that their login password will soon change to be their AD password, and that the **Username** in Movi 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 Movi if they do not upgrade.

   Add a message for Movi for Mac users: Mac-users will not get an upgrade prompt, they will have to download the new Movi 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 Cisco 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 Movi and old password will no longer work, that they need to use Movi 4.2 or later and their AD password and that the Movi **Username** must be configured as "<AD Short Domain Name>\username".

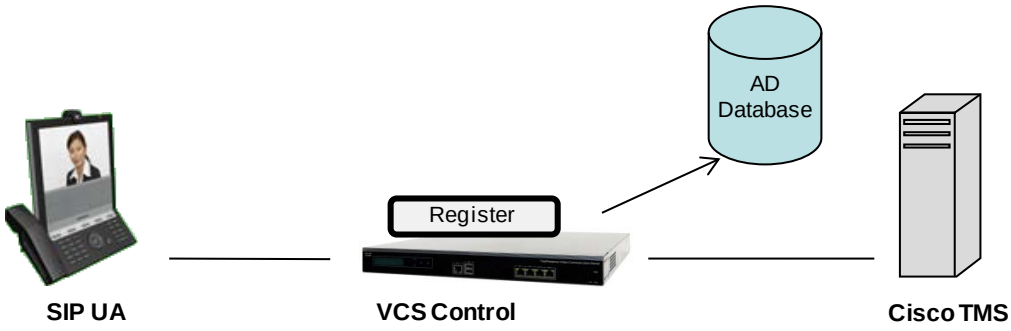
Appendix 12 — Example AD direct authentication deployments

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 on VCS Control
- VCS Control and VCS Expressway with Active Directory (direct) authentication for proxy registration

VCS Control with Active Directory (direct) authentication

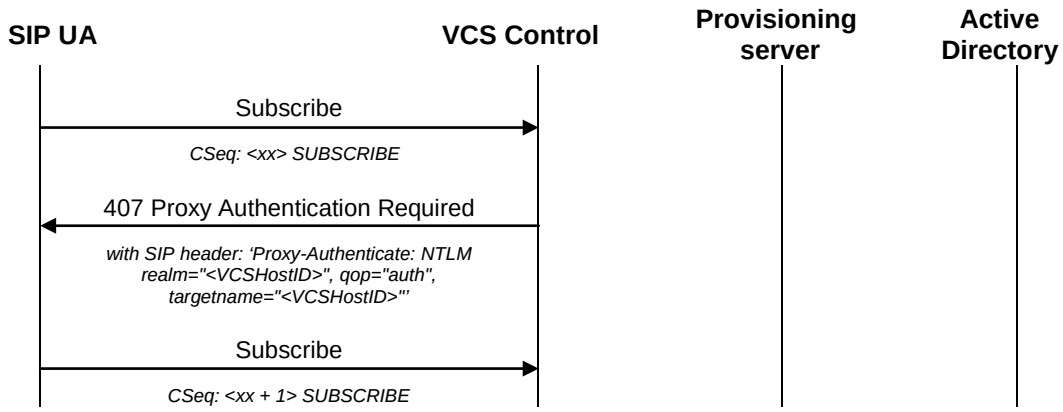
The SIP UA sends a request to the VCS Control and it challenges for authentication, sending the authentication details to the AD server for validation.

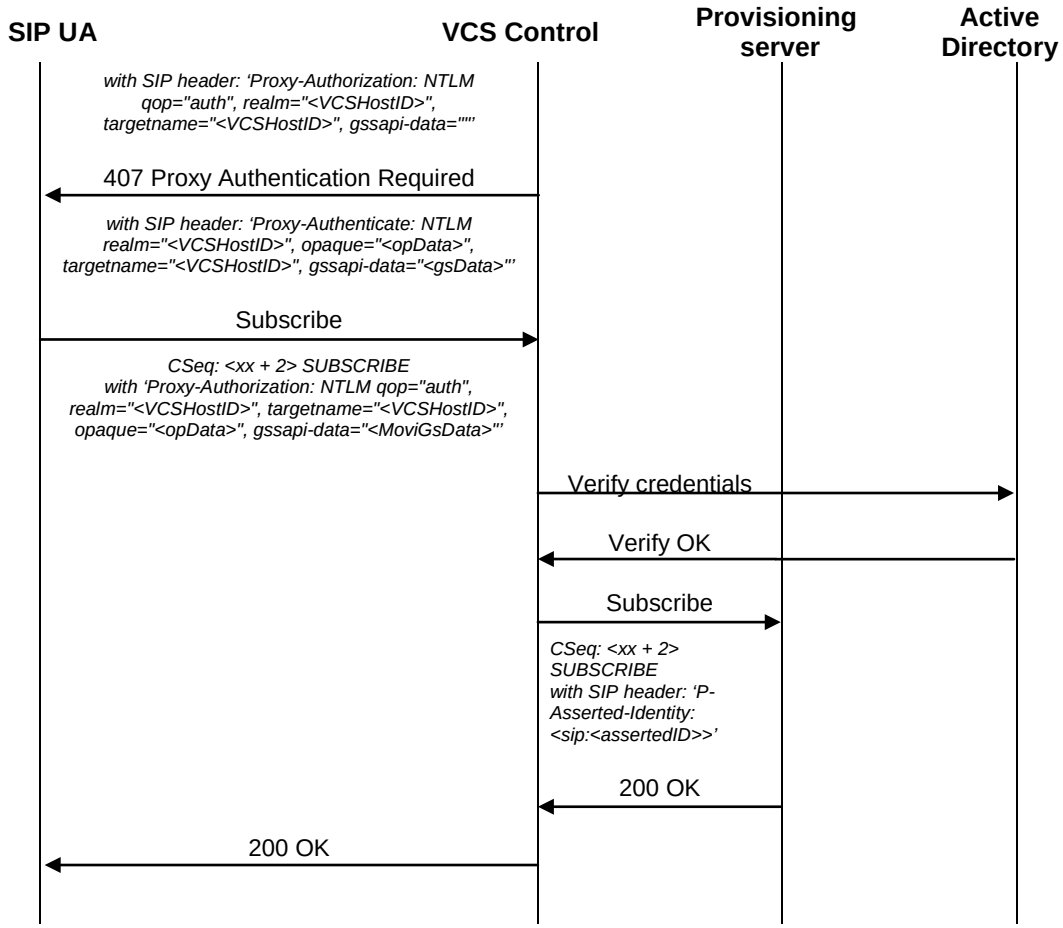


Setting	VCS Control
Provisioning	✓
AD configuration	✓
Default Zone	Check credentials
Default Subzone	Check credentials
SIP domain	Domain for SIP account

Setting	Cisco TMS
SIP Server	VCS Control IP address or FQDN

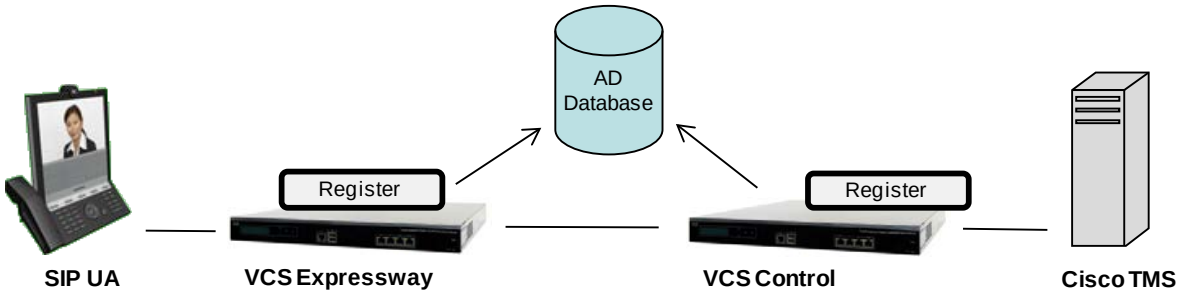
This example shows a subscribe for provisioning that is challenged using AD (direct) authentication:




SIP UA
VCS Control
Provisioning server
Active Directory
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

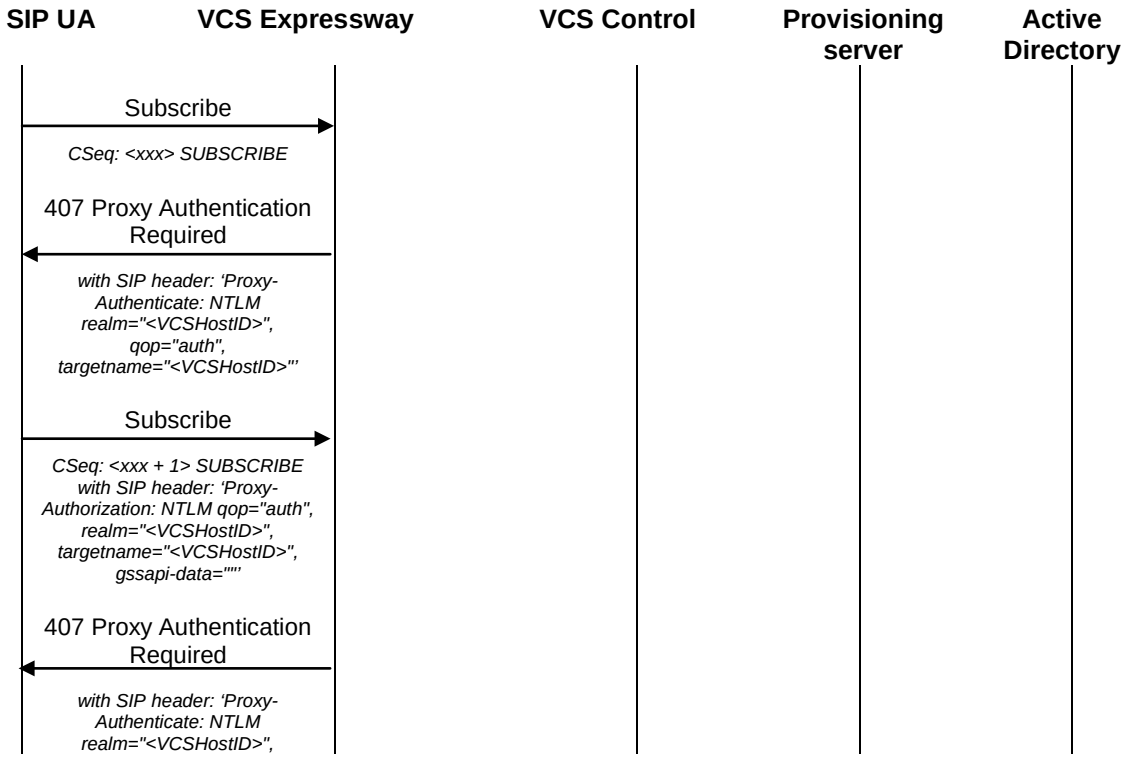
Both the VCS Expressway and the VCS Control can be configured to perform direct authentication against the AD server.

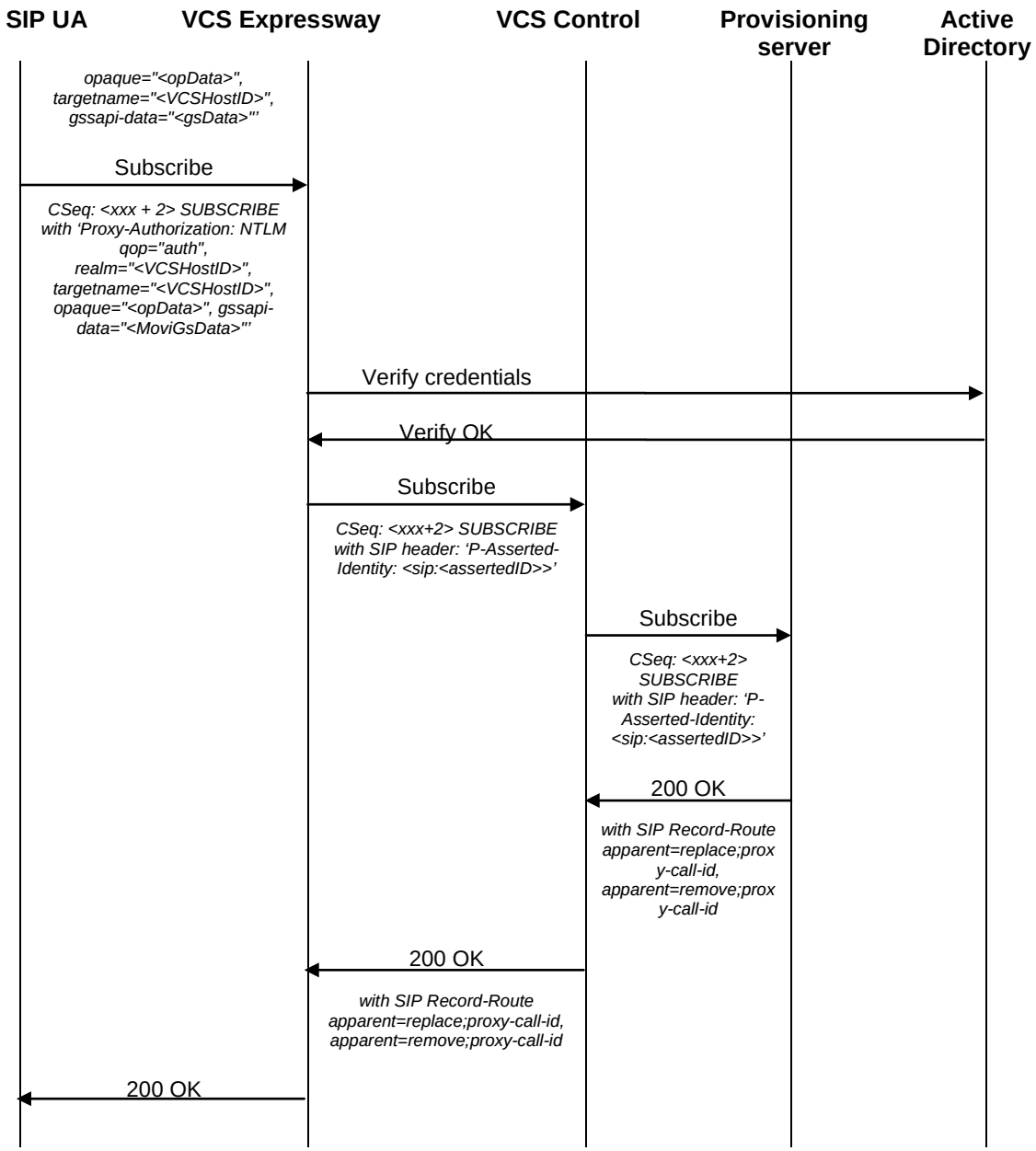


Setting	VCS Expressway	VCS Control
Provisioning	×	✓
AD configuration	✓	✓
Default Zone	Check credentials	Check credentials
Default Subzone	Check credentials	Check credentials
Traversal Zone	Check credentials	Check credentials
SIP domain	Domain for SIP account	Domain for SIP account
SIP registration proxy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

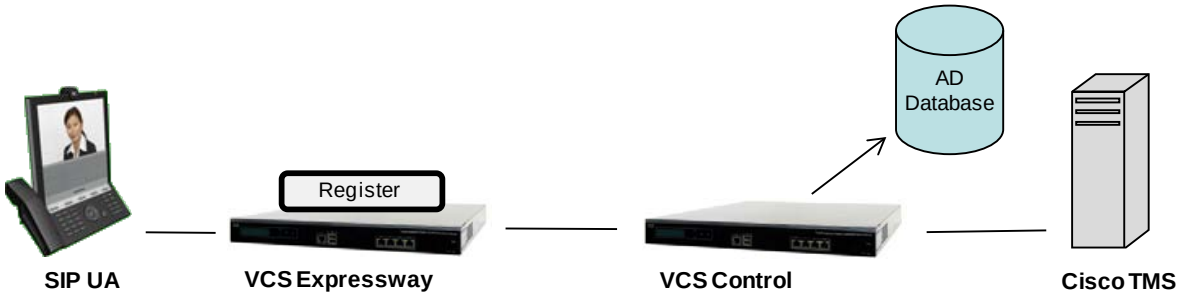



SIP UA
VCS Expressway
VCS Control
Provisioning server
Active Directory
opaque="<opData>", targetname="<VCSHostID>", gssapi-data="<gsData>"'
Subscribe
CSeq: <xxx + 2> SUBSCRIBE with 'Proxy-Authorization: NTLM qop="auth", realm="<VCSHostID>", targetname="<VCSHostID>", opaque="<opData>", gssapi-data="<MoviGsData>"'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

VCS Control and VCS Expressway with Active Directory (direct) authentication on VCS Control

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

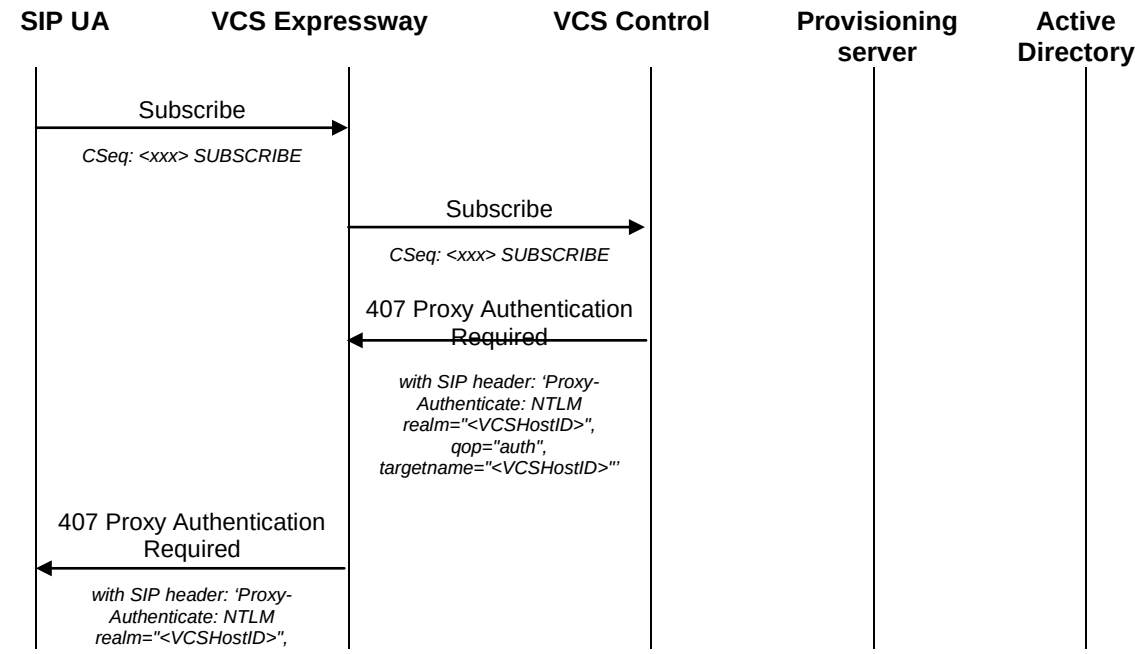
- The SIP UA sends a request to the VCS Expressway, but authentication does not happen until the request gets sent to the VCS Control.
- The registration takes place on the VCS Expressway, and as such is not authenticated. Provisioning requests, and call requests sent to the VCS Control will be challenged for authentication.

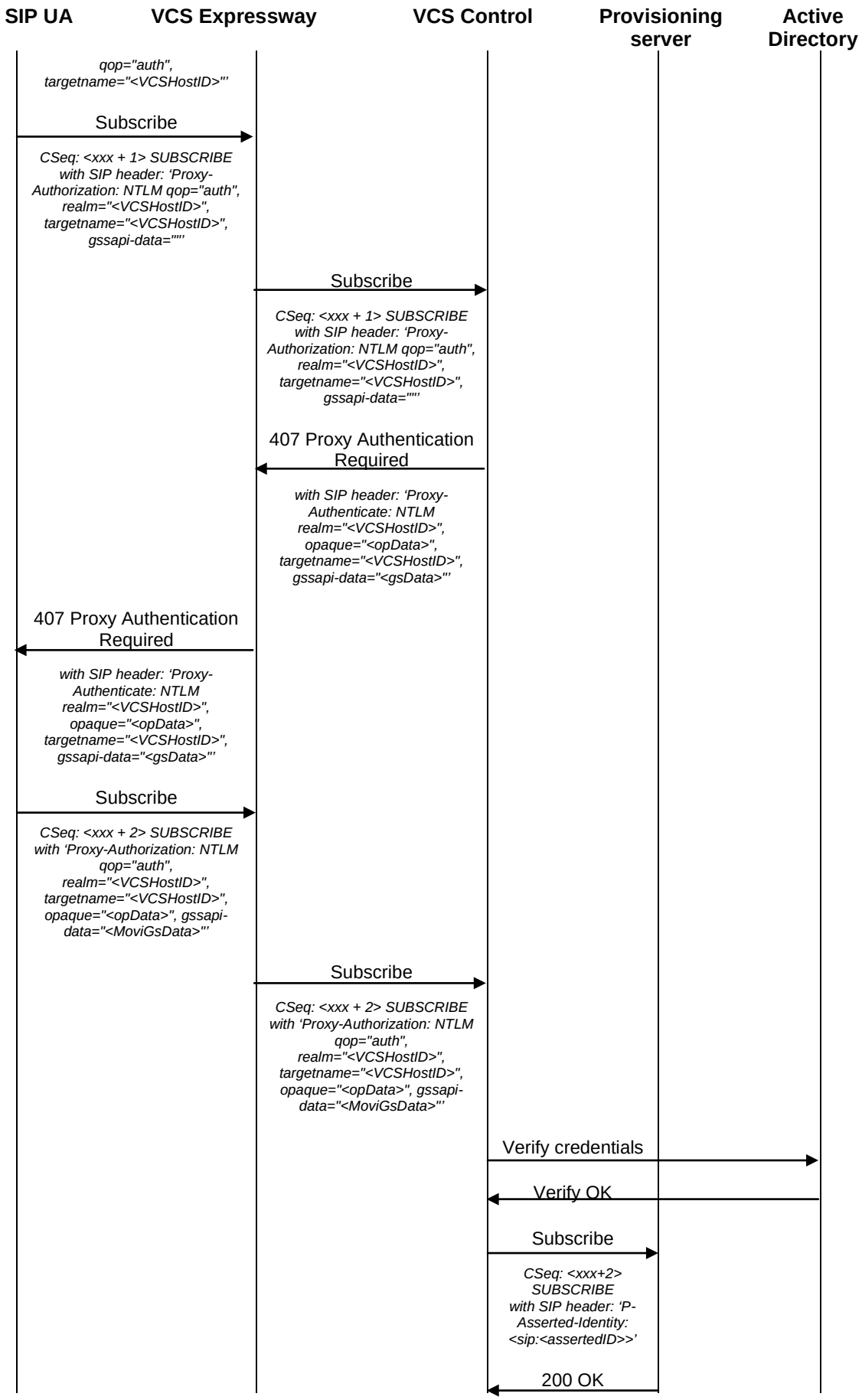


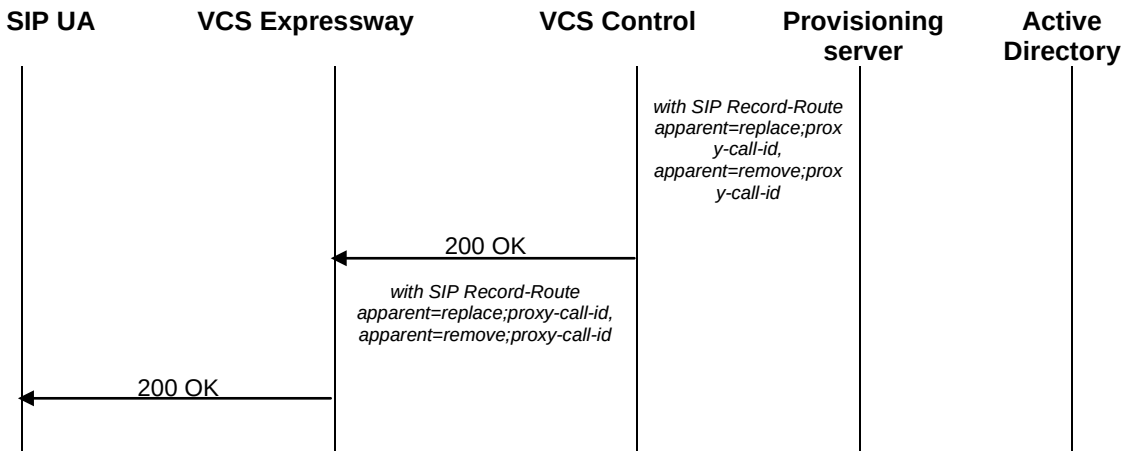
Setting	VCS Expressway	VCS Control
Provisioning	×	✓
AD configuration	×	✓
Default Zone	Do not check credentials	Check credentials
Default Subzone	Do not check credentials	Check credentials
Traversal Zone	Do not check credentials	Check credentials
SIP domain	Domain for SIP account	Domain for SIP account
SIP registration proxy mode	Off	Off

Setting	Cisco TMS
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 Control:



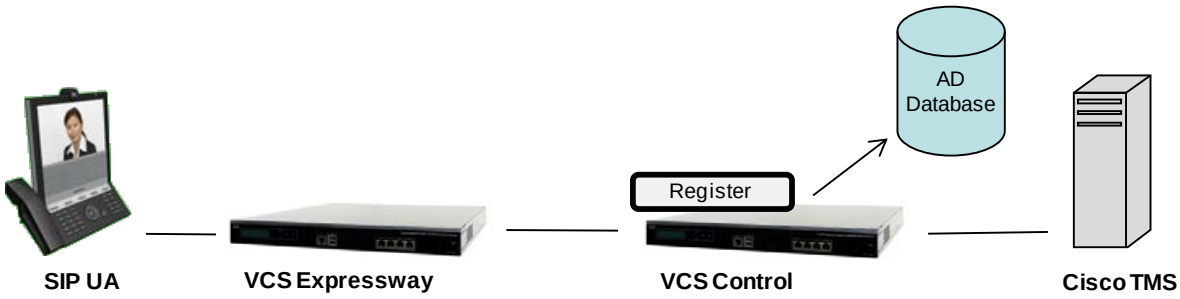

SIP UA
VCS Expressway
VCS Control
Provisioning server
Active Directory
qop="auth", targetname="<VCSHostID>"'
Subscribe
CSeq: <xxx + 1> SUBSCRIBE with SIP header: 'Proxy-Authorization: NTLM qop="auth", realm="<VCSHostID>", targetname="<VCSHostID>", gssapi-data=""'
Subscribe
CSeq: <xxx + 1> SUBSCRIBE with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


SIP UA
VCS Expressway
VCS Control
Provisioning server
Active Directory
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

VCS Control and VCS Expressway with Active Directory (direct) authentication for proxied registrations

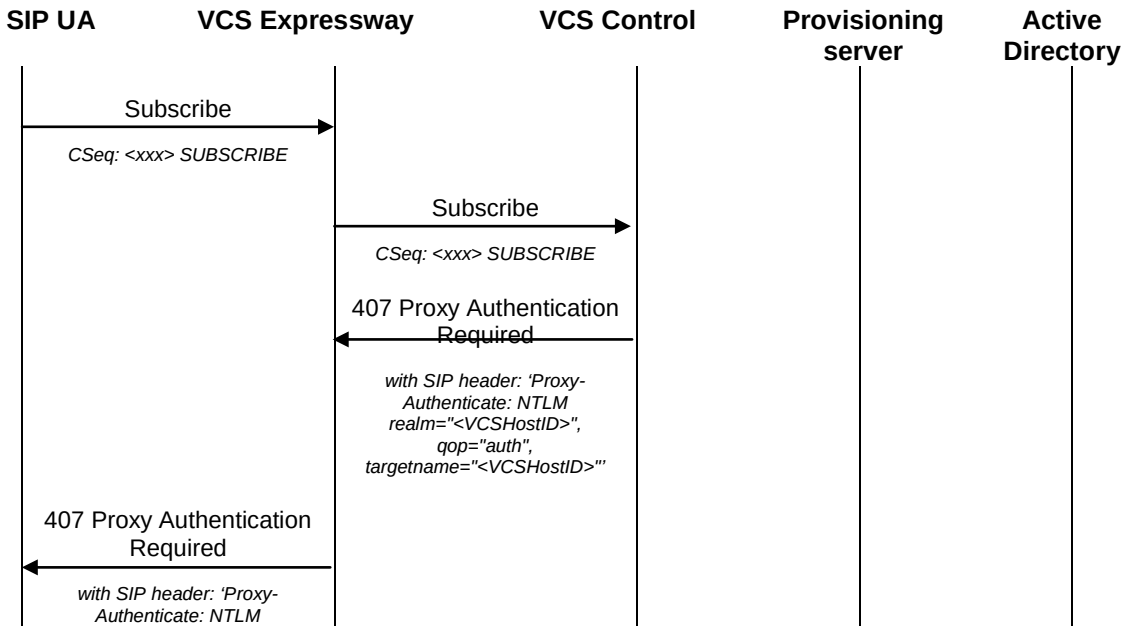
If the VCS Expressway cannot be connected directly to the AD server, then authentication can be performed on the VCS Control.

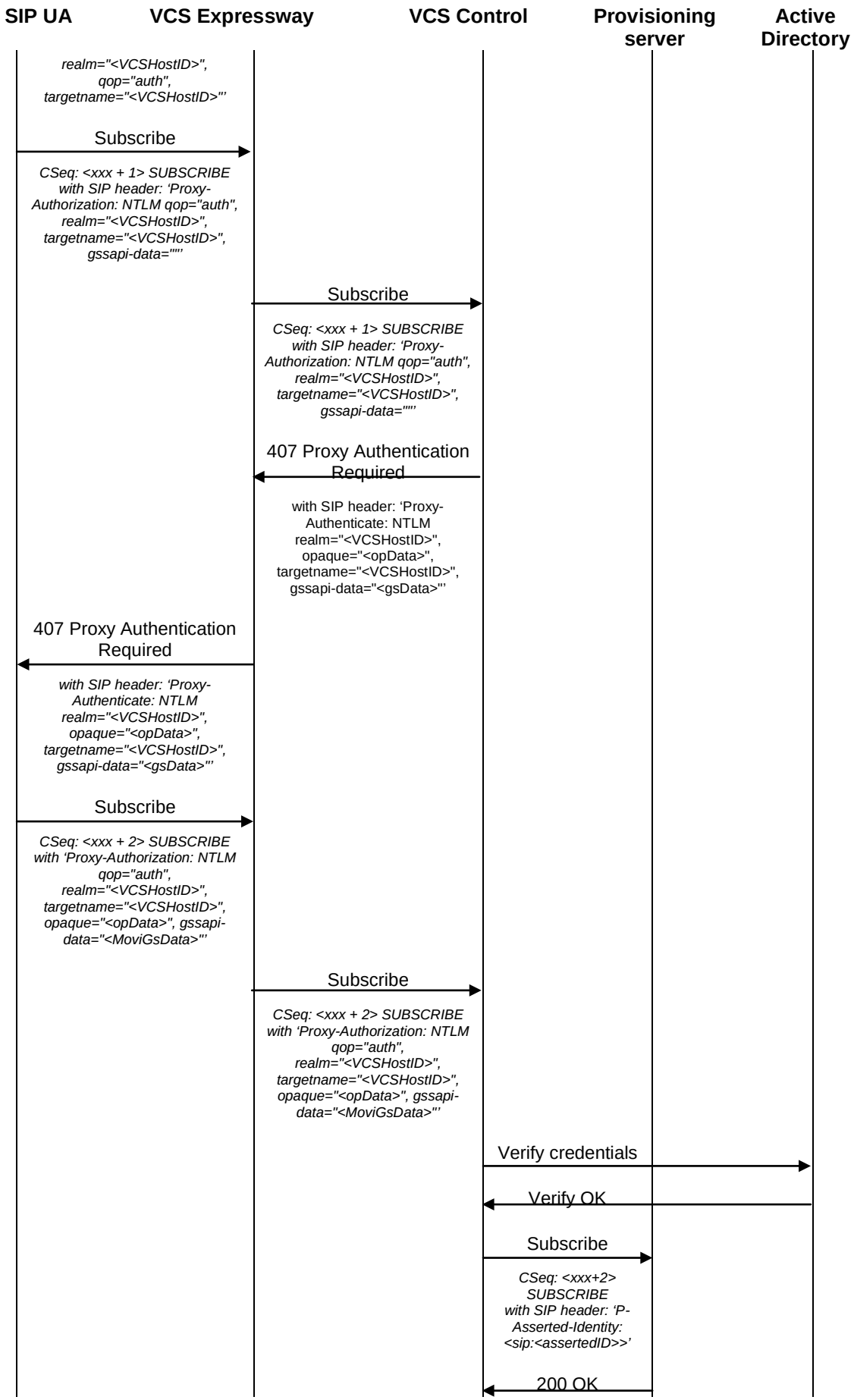
- The SIP UA sends a request to the VCS Expressway, but authentication does not happen until the request gets sent to the VCS Control.
- With proxied registrations the registration will occur on the VCS Control and will be challenged for authentication. Proxying registrations results in media traversing the firewall in more cases.

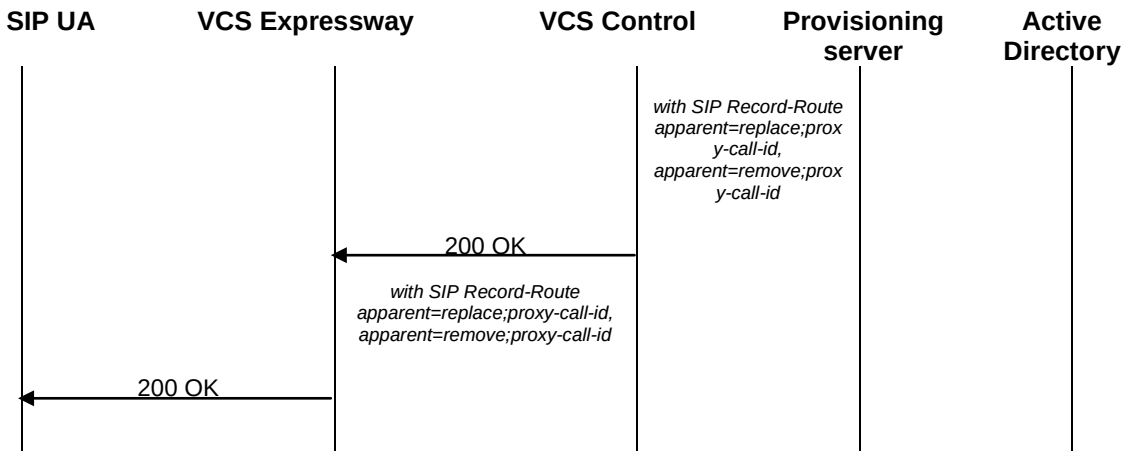


Setting	VCS Expressway	VCS Control
Provisioning	×	✓
AD configuration	×	✓
Default Zone	Do not check credentials	Check credentials
Default Subzone	Do not check credentials	Check credentials
Traversal Zone	Do not check credentials	Check credentials
SIP domain	-	Domain for SIP account
SIP registration proxy mode	Proxy to known only	Off

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




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


SIP UA
VCS Expressway
VCS Control
Provisioning server
Active Directory
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
1	May 2011	Initial release.
2	August 2011	Updated for Cisco VCS X7.0.
3	November 2011	Additional information on checking and setting NTLM versions on Movi PC.
4	February 2012	Added additional overview information on configuring authentication policy.
5	March 2012	Updated for Cisco VCS X7.1, including use of Cisco TMS Provisioning Extension mode.
6	August 2012	Updated for Cisco VCS X7.2