Authenticating Devices

Cisco TelePresence Deployment Guide

Cisco VCS X6.1

D14819.01

May 2011

Contents

Document revision history **4**

Introduction **5**

Local database **6**

Configuration 6

H.350 accessible database **7**

Configuration 7

Active Directory database (direct) **8**

Configuration 8
- Prerequisites 8
- IT request 8
- Configure Active Directory server details in VCS using the command line interface 9
- Configure Movi and test Active Directory database (direct) authentication 11

Appendix 1 – IT requisition **12**

H.350 accessible database: IT requisition (for H.350 LDAP access to database) 12
Active directory (direct): IT requisition (for access to Active Directory server) 13

Appendix 2 — SIP messages for a provisioning subscription **14**

Active Directory (direct) 14

Appendix 3 — Active Directory (direct): Example DNS SRV configuration for Active Directory **15**

DNS SRV values needed 15
Dig commands to check DNS SRV settings 15

Appendix 4 — Active Directory (direct): Checking and setting NTLM version on Movi **16**

Appendix 5 — IP Ports used on VCS for authentication **17**

H.350 accessible database 17
Active Directory (direct) 17

Appendix 6 — Troubleshooting **18**

Local database troubleshooting 18
H.350 accessible database troubleshooting 18
Active Directory (direct) troubleshooting 18
- Check password 18
- 401 unauthorized returned from the provisioning server to a SUBSCRIBE for provisioning 18
- Movi fails to authenticate due to a mismatch of NTLM versions 18
- PC fails to login following failed login attempts using AD direct authentication on a video endpoint 18

Appendix 7 – Active Directory (direct): Checking Domain information and VCS status **19**

Appendix 8 — Active Directory (direct): Leaving a Domain 20

Appendix 9 – Certificates for TLS 21

Appendix 10 – Use with Cisco VCS clusters 22

Active Directory (direct) 22

Appendix 11 — Example process for moving Movi users to AD direct authentication. 23

Document revision history

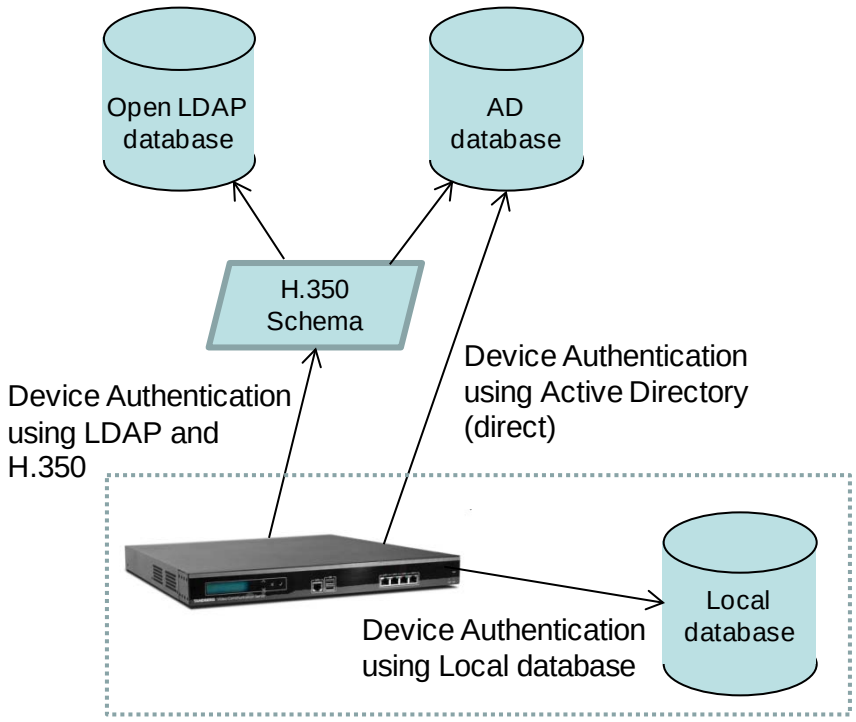
The following table summarizes the changes that have been applied to this document.

Revision	Date	Description
1	May 2011	Initial release.

Introduction

The Cisco TelePresence Video Communication Server (Cisco VCS) can be configured to support device authentication using either:

- an on-box local database of usernames and passwords
- real time access via LDAP to an external database which has an H.350 schema
- real time access to an Active Directory server using a Kerberos connection



Access to an Active Directory server using a Kerberos connection may be configured to work simultaneously with one of the other authentication methods. This is because the Active Directory server method is only supported by certain endpoints, such as the Cisco TelePresence Movi (version 4.2 and later).

This document describes how to configure the various methods of device authentication in Cisco VCS and how to configure the connections to the underlying authentication databases where applicable.

For all authentication methods, each endpoint is configured with a username and password that is used to match against credentials stored within the authentication database.

Local database

The **Local database** can be used for authenticating any endpoint, SIP and H.323.

It is hosted on the VCS unit and does not require any specific connectivity configuration.

Configuration

To use the Local database:

1. Go to **VCS configuration > Authentication > Devices > Configuration**.
2. Select *Local database* as the **Database type**.

The local database entries are configured on the **Local authentication database** page.

To enter a set of device credentials:

1. Go to **VCS configuration > Authentication > Devices > Local database**.
2. Click **New**.
3. Enter **Name** and **Password**.
4. Click **Create credential**.

H.350 accessible database

This can be used for authenticating any endpoint, SIP and H.323

Configuration

To use the H.350 accessible database:

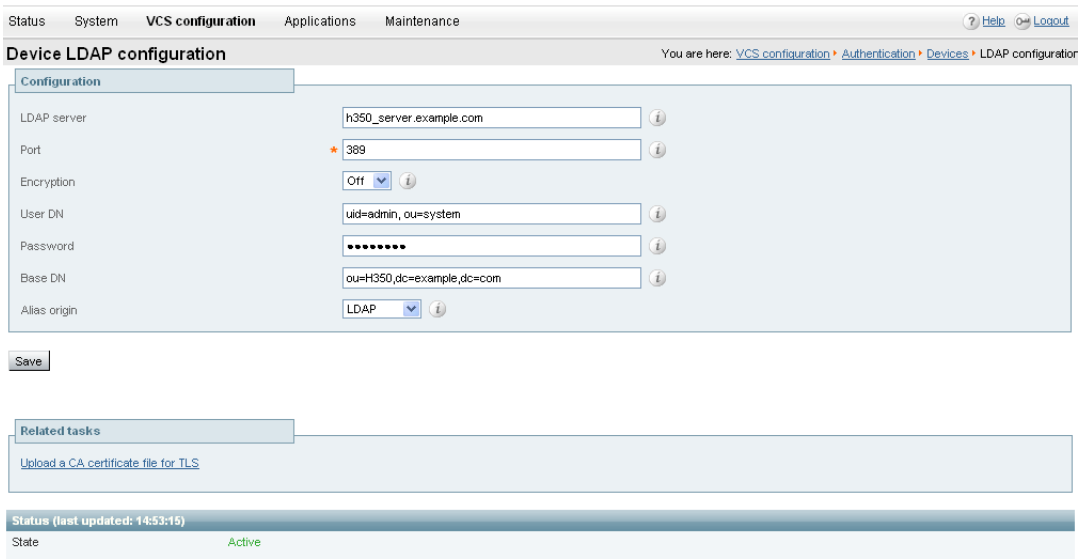
1. Go to **VCS configuration > Authentication > Devices > Configuration**.
2. Select *LDAP database* as the **Database type**.

To configure access to the H.350 database via LDAP:

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

LDAP server	<H.350 server IP address or domain>
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 **Security certificates** page (**Maintenance > Certificate management > Security certificates**). The default value is *Off*.
User DN	Distinguished name of username used when binding to the H.350 LDAP server (for example, uid=admin, ou=system)
Password	Password to use when binding to the H.350 LDAP server.
Base DN	Distinguished name to use when connecting to the H.350 LDAP server (for example, ou=H350,dc=example,dc=com).
Alias origin	This determines how aliases are checked and registered. The options are: *LDAP*: the aliases presented by the endpoint are checked against those listed in the LDAP database. *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 LDAP database. The default value is *LDAP*.

Connection is successful when the Status reports State Active



Active Directory database (direct)

Currently, Active Directory database (direct) authentication can only be used by Movi version 4.2 or later. It can be enabled at the same time as either the local or H.350 accessible databases.

If enabled on the Cisco VCS, Movi 4.2 and later will automatically use this instead of other methods of authentication (other devices will be authenticated by the other chosen authentication method).

The Cisco VCS must be configured to challenge for authentication on the relevant zones and subzones (the Default Zone for provisioning, and the relevant subzone for registrations and call authentication). Note that Active Directory database (direct) authentication is only supported by VCS challenges, and not by provisioning server (TMS Agent) challenges.

Note: This document does not specify the configuration of Cisco VCS and Cisco TMS to enable provisioning. For details about configuring provisioning, see the *Cisco TMS Provisioning Deployment Guide* (document D14368) and the *Cisco TMS Provisioning Troubleshooting Guide* (document D14427).

Configuration

Prerequisites

Active Directory

- 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 must all be in a single AD domain.
- A username and password of an AD user with either “account operator” or “administrator” access rights must be available for the Cisco VCS to use for joining and leaving the domain.

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 to be used to identify the AD server in VCS, the DNS server must be configured accordingly.

Cisco VCS

- If using DNS to identify the AD server, the VCS must be configured to use that DNS server (**VCS configuration > DNS**).
  - The VCS’s **Local host name** must be 15 or less characters long.
  - When part of a cluster, ensure that each Cisco VCS peer has a unique **Local host name**.
- Ensure that an NTP server (**VCS configuration > Time**) has been configured and is active.

Endpoint

- The PC on which Movi runs must use NTLMv2 or later (see Appendix 4 — Active directory (direct): Checking and setting NTLM version on Movi PC).

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 VCS using the command line interface

In VCS X6.1, the configuration of Active Directory (direct) can only be performed using the command line interface (CLI):

1. Log in as admin over SSH or via the serial interface, then type:
   a. xConfiguration Authentication ADS ADDomain: <AD DOMAIN (FQDN) in CAPITALS>
   b. xConfiguration Authentication ADS Workgroup: <AD Short Domain Name>
   <AD Short Domain Name> is also known as <NetBIOS Domain Name>
2. The following parameters may also optionally be configured (typically these values can be left at their default settings).

Command	Values	Comment
xConfiguration Authentication ADS SecureChannel	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*.
xConfiguration Authentication ADS 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 > Security certificates**). The default value is *TLS*.
xConfiguration Authentication ADS Clockskew	<Skew value in seconds>	This sets up the maximum clock skew allowed between the VCS and the KDC (Kerberos Key Distribution Center). Generally this should be left at its default value: 300 (5 minutes). **Note**: ensure that VCS and KDC are synchronized to time servers.
xConfiguration Authentication ADS SPNEGO	Enabled / Disabled	This enables or disables the “Simple and Protected GSSAPI Negotiation Mechanism” to identify authentication protocols that can be used between VCS and the AD domain controller. Generally this should be left at its default value: *Enabled*

3. Configure the Primary Domain Controller server address.

Note: This step is only required if the DNS SRV lookup of “Authentication ADS ADDomain” does not provide the list of Domain Controller servers.

- `xcommand AdsDcAdd <PDC IP address>`
  where <PDC IP address> is the IP address of the Primary Domain Controller server.

4. Configure the Primary Kerberos Key Distribution Center server address.

Note: This step is only required if the DNS SRV lookup of “Authentication ADS ADDomain” does not provide the list of Kerberos Key Distribution Center servers.

- `xcommand AdsKdcAdd <PKKDC IP address>`

  or if the port number is not 88:
  `xcommand AdsKdcAdd <PKKDC IP address> <IP port>`

where <PKKDC IP address> is the IP address of the Primary Kerberos Key Distribution Center server
and <IP port> is the IP port of the Primary Kerberos Key Distribution Center server.

Note: Key Distribution Center addresses are typically the same as the Domain Controller addresses

5. Enable the Cisco VCS to join the domain and offer Active Directory database (direct) authentication. Type:
   - xConfiguration Authentication ADS Mode: On

Join the Cisco VCS into the AD Domain

Note: for clusters, the Join Domain process must be carried out on every peer in the cluster

To join the VCS into the AD domain, access to VCS via the root login is required.

1. Login as root over SSH or via the serial interface, then:
   a. Type `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 1) Join 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 Join will result in the messages:

  ```
  Using short domain name -- <AD Short Domain Name>
  Joined '<DNS Local hostname>' to realm '<AD DOMAIN (FQDN)>'
  …
  Domain join succeeded
  ```

- An unsuccessful Join will result in an error message, for example:

  ```
  "Error message:
  failed to kinit password: NT_STATUS_UNSUCCESSFUL
  Domain join failures
  Failures to join the domain may be caused by being unable to contact
  the domain server, or due to certificate or credential failures."
  ```

  Check that the configuration, certificate, the username and password have been entered correctly.

Note: you only need to Join the VCS to AD domain once, even if ADS mode is turned off and on again. The only time a Join will be needed again is if a Leave of the domain is performed, or you need to Join a different domain.

Add non primary Domain Controllers and Kerberos Key Distribution Center servers

1. Configure the Domain Controller server addresses if required.

   Note: This step is only required if the DNS SRV lookup of "Authentication ADS ADDomain" does not provide the list of Domain Controller servers.

   Up to four further Domain Controller server addresses (up to 5 in total) can now be added. Only do this if the Primary Domain Controller server address was entered earlier. For each additional Domain Controller server type:

   - `xcommand AdsDcAdd <IP address>`
     where <IP address> is the IP address of the non-primary Domain Controller server.
2. Configure the Kerberos Key Distribution Center server addresses.

   Note: This step is only required if the DNS SRV lookup of "Authentication ADS ADDomain" does not provide the list of Kerberos Key Distribution Center servers.

   Up to four further Kerberos Key Distribution Center server addresses (up to 5 in total) can now be added. Only do this if the Primary Kerberos Key Distribution Center server address was entered earlier. For each additional Kerberos Key Distribution Center server type:

   - `xcommand AdsKdcAdd <IP address>`

     or if the port number is not 88:
     `xcommand AdsKdcAdd <IP address> <IP port>`

     where <IP address> is the IP address of the non-primary Kerberos Key Distribution Center server
     and <IP port> is the IP port of the Kerberos Key Distribution Center server at this IP.

   Note: Key Distribution Center addresses are typically the same as the Domain Controller addresses

Enable NTLM authentication challenges

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

- xConfiguration SIP Authentication NTLM mode: Auto

  Other options for this mode are *Off* and *On*. Never use *On*, as this will send NTLM challenges to devices that may not support NTLM (and therefore they may crash or otherwise misbehave).

Configure Movi and test Active Directory database (direct) authentication

You are recommended to use a Movi configuration that already authenticates successfully using either provisioning or Cisco 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:
   - In the **Username** field, configure <AD Short Domain Name>\username
     (this field is not case sensitive).
   - 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 – IT requisition

H.350 accessible database: IT requisition (for H.350 LDAP access to database)

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 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.

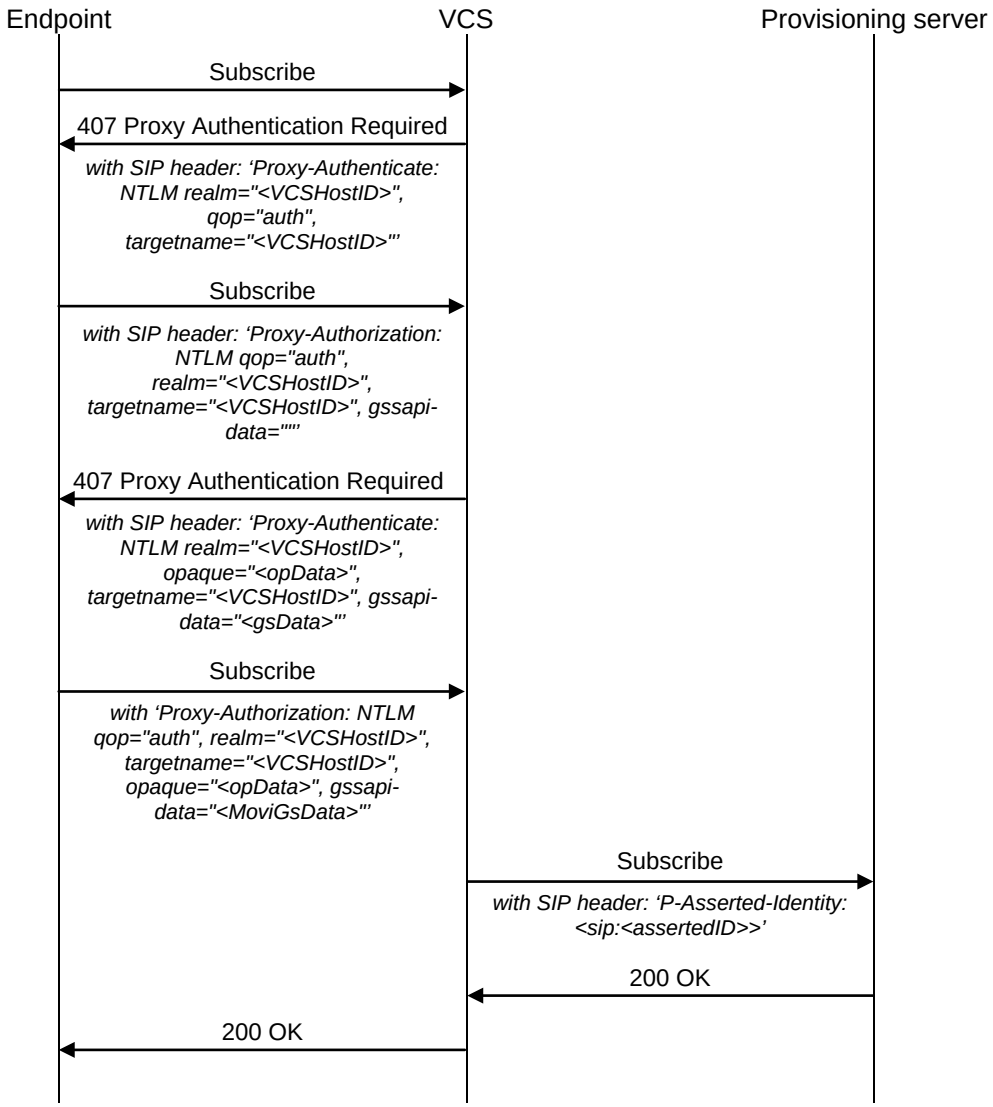
Active Directory Domain (FQDN)	
Active Directory Short Domain Name (NetBIOS Domain Name)	
Is a secure channel required between VCS and the AD domain controller?	YES / NO
Is TLS encryption needed between VCS and the AD server? Certificate location?	YES / NO Path to certificate file:
Is a clock skew value 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 2 — 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 3 — Active Directory (direct): Example DNS SRV configuration for Active Directory

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.

Dig commands 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 4 — Active Directory (direct): Checking and setting NTLM version on Movi

Active Directory direct requires NTLMv2, but some Windows PCs (for example, Windows XP PCs) may be configured to use NTLMv1. If this is the case the authentication will fail and it may be hard to diagnose as there will be no analysis or warnings on the Cisco VCS, as the Cisco VCS just passes the authentication request through to the AD server.

In Windows registry, check to see if there is a setting called “LmCompatibilityLevel”; this entry controls the negotiation of NTLM versions.

Note: This setting does not exist and does not need checking in Windows 7.

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

- The key called LmCompatibilityLevel (REG_DWORD) needs to be set to a value of 2 or higher.
- The meanings of the values in LmCompatibilityLevel are explained in: http://technet.microsoft.com/en-us/library/cc960646.aspx

Appendix 5 — IP Ports used on VCS for authentication

H.350 accessible database

The following table lists the ports used for device authentication between VCS and the H.350 accessible database:

VCS port	Destination port	Usage
TCP/40000 .. 49999	TCP/389	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	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 6 — Troubleshooting

Local database troubleshooting

No specific troubleshooting.

H.350 accessible database 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 fails to authenticate due to a mismatch of NTLM versions

In order to use Active Directory (direct) mode, the PC running Movi must be using NTLMv2 or later. To check (and change if required), the version of NTLM running on the PC see “Appendix 4 — Active directory (direct): Checking and setting NTLM version on Movi PC”.

PC fails to login following failed login attempts using AD direct authentication on a video endpoint

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.

Appendix 7 – Active Directory (direct): Checking Domain information and VCS status

Note: For clusters, each peer can be checked.

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 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
```

   c. Choose option 3) VCS Status
   d. When asked, enter the domain administrator username
   e. 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.

- The VCS will report:

```
… Lots of details …

Domain status request succeeded
```

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 using an OCS server are described in the Cisco VCS deployment guide "*Certificate creation and use with Cisco VCS*" (document reference D14548).

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 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 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 the Movi 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".

   Note: 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.

   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 NTLM, but leave **SIP Authentication NTLM mode** as *Off*.
5. When ready to switch over:
   a. Set **SIP Authentication NTLM mode** to *Auto*.
   b. Set up *Check Credentials* on the Cisco VCS Default Zone.
6. Send out a reminder e-mail 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".