Contents

Introduction ......................................................................................................................... 3
Usage ........................................................................................................................................ 3

VCS configuration.................................................................................................................. 4
Configure LDAP server details on VCS ............................................................................ 4
  Status messages on the Login account LDAP configuration page .................................. 6
Configure DNS server ........................................................................................................... 6
Define groups on VCS .......................................................................................................... 7
  Groups for administrator login .......................................................................................... 7
  Groups for user login ......................................................................................................... 8
Define groups in the authentication server ......................................................................... 8
Set login authentication to use remote database ................................................................. 8

Appendix 1 – IT requisition (for access to authentication server) ....................................... 10
Appendix 2 – IT requisition (for group configuration) ......................................................... 11
Appendix 3 – Active Directory structure ............................................................................ 12
Appendix 4 – Configuring groups in Active Directory ....................................................... 14
  Create a group object ........................................................................................................ 14
  Make a user a member of a group .................................................................................... 15

Appendix 5 – Troubleshooting ............................................................................................ 16
  Viewing / searching LDAP database ............................................................................... 16
  Unable to log in after switching to remote authentication ............................................... 16
  AD “Domain Users” group fails to allow login ................................................................. 16

Appendix 6 – Certificates for TLS ....................................................................................... 17
Appendix 7 – Use with VCS clusters ................................................................................... 18
Document revision history ................................................................................................. 19
Introduction

Increasingly, users have to supply authentication credentials (usernames and passwords) in order to log in to devices and systems. Rather than having to remember separate usernames and passwords for each device, it is easier and more preferable for users to have a single set of sign-in credentials that are managed centrally by an LDAP accessible server.

The device being accessed, rather than looking up the username and password in its own internal database, contacts the LDAP accessible server to both authenticate the user and also to check whether that authenticated user belongs to a group that the device authorizes to perform the functionality requested.

Using a central login credential database also allows the company to define policies for passwords, such as the replacement interval, level of complexity and so on, and be sure that it applies to passwords for all systems.

This document describes how to configure the Cisco TelePresence Video Communication Server (Cisco VCS) to authenticate login accounts over LDAP.

LDAP authentication and authorization is used for web login to the Cisco VCS’s administrator and user (FindMe) accounts.

Currently, Windows Active Directory is the only LDAP accessible server supported by the VCS.

Note that:
- Other logins, including serial, Telnet and SSH continue to use the admin account configured on the VCS.
- User account web login only applies if device provisioning is in TMS Agent legacy mode, or you are using FindMe without TMS.

Usage

As an operator you will need to:
- have users, together with passwords, configured in the LDAP accessible server
- configure groups in the LDAP accessible server which define capabilities of the users
- associate users with groups in the LDAP accessible server
- configure VCS for LDAP operation

A user, logging in to the VCS for administrator access or to configure FindMe (depending on how the VCS has been configured) will be authenticated using the LDAP server credentials.

Both the username and password are case sensitive.
VCS configuration

Configure LDAP server details on VCS

1. Go to the Login account LDAP configuration page (Maintenance > Login accounts > LDAP configuration).
2. Configure the following fields so that the VCS can connect to the LDAP server to authenticate login accounts and check group membership (you can use the questionnaire in Appendix 1 – IT requisition (for access to authentication server) to get the appropriate information from your IT department):

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server address</td>
<td>Fully Qualified Domain Name of the LDAP server (case insensitive) or the IP address of the LDAP server. If using TLS, the server address entered here must match the CN (common name) contained within the certificate presented by the LDAP server.</td>
</tr>
<tr>
<td>FQDN address resolution</td>
<td>Address Record: if the Server address above is not an IP address, look the value up as an IPv4 DNS A record, or an IPv6 DNS AAAA record. SRV Record: if the Server address above is not an IP address, look the value up as a DNS SRV record.</td>
</tr>
<tr>
<td>Port</td>
<td>IP port to use on the LDAP server, typically 389 if encryption is off, and 636 if encryption is set to TLS.</td>
</tr>
<tr>
<td>Encryption</td>
<td>If the LDAP server supports TLS encryption, set this to TLS; otherwise set it to Off. Note: if encryption is set to TLS, a valid CA certificate, private key and server certificate must be uploaded to VCS in the Security certificates page (Maintenance &gt; Security certificates).</td>
</tr>
</tbody>
</table>
| Certificate revocation list (CRL) checking | Only applicable if Encryption is TLS.  
None: CRLs are not to be checked.  
Peer: only the CRL directly associated with the Certificate Authority that issued the LDAP server’s certificate is checked.  
All: CRLs of all the Certificate Authorities in the trust chain of the LDAP server’s certificate are checked. |
| VCS bind DN                    | cn=, ou= and dc= definition of the account object that will allow the VCS to query the database (case insensitive) – See Appendix 3 – Active Directory structure. It is important to specify the DN in the order cn=, then ou=, then dc=. |
| VCS bind password              | Password of the account object that the VCS will use to query the database (case sensitive). |
| SASL                           | Enable Simple Authentication and Security Layer if it is company policy to do so. |
| VCS bind username              | Username of the account that the VCS will use to log in to the LDAP server (case sensitive). Only required if SASL is enabled – configure this to be the sAMAccountName; Security Access Manager Account Name (in AD this is the Account’s user logon name). |
| Base DN for accounts           | ou= and dc= definition of the Distinguished Name where a search for user accounts should start in the database structure (case insensitive). This is for authentication of both administrator login and user login requests. It is important to specify the DN in the order ou=, then dc=. |
| Base DN for groups             | ou= and dc= definition of the Distinguished Name where a search for groups should start in the database structure (case insensitive). This is for authorization of an authenticated user to log in as an administrator or to log in to a user account. It is important to specify the DN in the order ou=, then dc=. |

Note that:
- The VCS Bind account is usually a read-only account with no special privileges.
The Base DN for accounts and groups must be at or below the dc level (include all dc= values and ou= values if necessary). LDAP authentication does not look into sub dc accounts, only lower ou= and cn= levels.

For example, using the values from Appendix 3 – Active Directory structure:

<table>
<thead>
<tr>
<th>Server address</th>
<th>servercluster1.corporation.int</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN address resolution</td>
<td>SRV Record</td>
</tr>
<tr>
<td>Port</td>
<td>389 (this is the default value and cannot be changed for SRV Record address resolution)</td>
</tr>
<tr>
<td>Encryption</td>
<td>Off (or TLS … if TLS, ensure the relevant certificates are loaded)</td>
</tr>
<tr>
<td>Certificate revocation list (CRL) checking</td>
<td>None</td>
</tr>
<tr>
<td>VCS bind DN</td>
<td>cn=vcs,ou=sys,ou=region1,ou=accounts,dc=corporation,dc=int</td>
</tr>
<tr>
<td>VCS bind password</td>
<td>&lt;password for VCS account&gt;</td>
</tr>
<tr>
<td>SASL</td>
<td>DIGEST-MD5 (or None)</td>
</tr>
<tr>
<td>VCS bind username</td>
<td>VCS</td>
</tr>
<tr>
<td>Base DN for accounts</td>
<td>ou=region1,ou=accounts,dc=corporation,dc=int</td>
</tr>
<tr>
<td>Base DN for groups</td>
<td>ou=groups,dc=corporation,dc=int</td>
</tr>
</tbody>
</table>
Status messages on the Login account LDAP configuration page

State = Active
No error messages are displayed.

State = Failed
The following error messages may be displayed:

<table>
<thead>
<tr>
<th>Error message</th>
<th>Reason / resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS unable to do reverse lookup</td>
<td>Reverse DNS lookup is required for SASL authentication.</td>
</tr>
<tr>
<td>DNS unable to resolve LDAP server address</td>
<td>Check that a valid DNS server is configured, and check the spelling of the LDAP server address.</td>
</tr>
<tr>
<td>Failed to connect to LDAP server. Check server address and port</td>
<td>Check that the LDAP server details are correct.</td>
</tr>
<tr>
<td>Failed to setup TLS connection. Check your CA certificate</td>
<td>CA certificate, private key and server certificate are required for TLS.</td>
</tr>
<tr>
<td>Failure connecting to server. Returned code&lt;return code&gt;</td>
<td>Other non-specific problem.</td>
</tr>
<tr>
<td>Invalid Base DN for accounts</td>
<td>Check Base DN for accounts; the current value does not describe a valid part of the LDAP directory.</td>
</tr>
<tr>
<td>Invalid server name or DNS failure</td>
<td>DNS resolution of the LDAP server name is failing.</td>
</tr>
<tr>
<td>Invalid VCS bind credentials</td>
<td>Check VCS Bind DN and VCS Bind password, this error can also be displayed if SASL is set to DIGEST-MD5 when it should be set to None.</td>
</tr>
<tr>
<td>Invalid VCS bind DN</td>
<td>Check VCS Bind DN; the current value does not describe a valid account in the LDAP directory. This Failed state may be wrongly reported if the VCS bind DN is 74 or more characters in length. To check whether there is a real failure or not, set up an administrator group or user group on the VCS using a valid group name. If VCS reports “saved” then there is not a problem (the VCS checks that it can find the group specified). If it reports that the group cannot be found then either the VCS bind DN is wrong, the group is wrong or one of the other configuration items may be wrong.</td>
</tr>
<tr>
<td>There is no CA certificate installed</td>
<td>CA certificate, private key and server certificate are required for TLS.</td>
</tr>
<tr>
<td>Unable to get configuration</td>
<td>LDAP server information may be missing or incorrect.</td>
</tr>
</tbody>
</table>

Configure DNS server

Ensure one or more DNS server addresses are set up on the VCS (System > DNS).

Note: If SASL is enabled the DNS servers must support reverse DNS lookup.

DNS is required for:
- Finding the IP address of the LDAP server if the server is defined by name rather than IP address.
- If SASL is enabled, part of the security process is to perform an IP address to name check – a reverse DNS lookup for that LDAP server.
Define groups on VCS

In the LDAP accessible database, groups are assigned to users to give them specific capabilities. The same groups must be defined on the VCS and configured with the required authorization levels for VCS access.

Groups for administrator login

1. Go to the Administrator groups page (Maintenance > Login accounts > Administrator groups).
   At this stage, ignore the warning “Warning: These groups are not active. To use these groups you must set the Administrator authentication source to Remote or Both.” – this will be configured later.
2. Click New.
3. Configure the fields as follows:
   
<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the group name to be used for the type of account required, for example VCS_admin_RW – for writeable access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access level</td>
<td>Select the appropriate entry:</td>
</tr>
<tr>
<td></td>
<td>Read-write: if writeable access is required.</td>
</tr>
<tr>
<td></td>
<td>Read-only: if read-only access is required.</td>
</tr>
<tr>
<td></td>
<td>Auditor: if access only to Event Log, Configuration Log and the Overview page are to be allowed.</td>
</tr>
<tr>
<td>Web access</td>
<td>Select Yes.</td>
</tr>
<tr>
<td>API access</td>
<td>This controls access to the XML and REST APIs by systems such as Cisco TMS. Select Yes if members of this group need to access the system’s APIs.</td>
</tr>
<tr>
<td>State</td>
<td>Select Enabled.</td>
</tr>
</tbody>
</table>

4. Click Save.

Note:
- Access levels are prioritized so that if an administrator user is found in more than one group, it is assigned the highest level permission for each of the access settings across all of its groups.
- A warning is displayed at the top of the Administrator groups page if a group name cannot be found.
When configured and operating, the user name that must be used to log into the VCS is the sAMAccountName; Security Access Manager Account Name (in AD the account’s user logon name).

**Groups for user login**

Note that user account web login only applies if device provisioning is in TMS Agent legacy mode, or you are using FindMe without TMS.

1. Go to the User groups page (Maintenance > Login accounts > User groups).

   **Note:** At this stage, ignore the warning “Warning: These groups are not active. To use these groups you must set the user authentication source to Remote.” – this will be configured later.

2. Click **New**.

3. Configure the fields as follows:

   | Name       | Enter the group name to be used for a read/write account, e.g. VCS_User  
   |------------|---------------------------------------------------------------------  
   | State      | Select *Enabled*.  

4. Click **Save**.

   Note that a warning is displayed at the top of the Administrator groups page if a group name cannot be found.

   The login user name that must be used to log into the user account is the sAMAccountName; Security Access Manager Account Name (in AD this is the account’s user logon name).

**Define groups in the authentication server**

Defining groups in the authentication server is usually carried out by the IT department; use copies of Appendix 2 – IT requisition (for group configuration) to request your IT department to set up the relevant groups and assign users to those groups.

You are likely to want to set up the following groups:

- Read-write administrator (for example, group VCS_admin_RW)
- Read-only administrator (for example, group VCS_admin_RO)
- Auditor administrator (for example, group VCS_auditor)
- VCS user (for example, group VCS_User)

**Set login authentication to use remote database**

1. Go to the Login account authentication configuration page (Maintenance > Login accounts > Configuration).

2. Configure the fields as follows:
3. Click **Save**.
Appendix 1 – IT requisition (for access to authentication server)

To: IT Department

Please supply the following details so that the Cisco VCS can be configured to access the LDAP server to authenticate and authorize login users.

For access authorization, VCS will look for users in the groups:
- __________________________ to allow them Read / Write access for administrator login
- __________________________ to allow them Read Only access for administrator login
- __________________________ to allow them Read / Write access for user login

<table>
<thead>
<tr>
<th>LDAP server</th>
<th>- Fully Qualified Domain or IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>If FQDN is it an A / AAAA record or SRV record?</td>
<td>A or AAAA / SRV</td>
</tr>
<tr>
<td>Port</td>
<td>- IP port for the LDAP server (typically 389 or 636)</td>
</tr>
<tr>
<td>Encryption</td>
<td>- Use TLS encryption to access the LDAP server?</td>
</tr>
<tr>
<td>Certificate location?</td>
<td>- Path to certificate file:</td>
</tr>
<tr>
<td>Certificate revocation list</td>
<td>- No checking / Check single CA / Check all CAs in trust chain</td>
</tr>
<tr>
<td>VCS bind DN</td>
<td>- location of the VCS account object, including all cn=,ou=,dc= fields</td>
</tr>
<tr>
<td>VCS bind password</td>
<td>- password for the VCS login account</td>
</tr>
<tr>
<td>SASL</td>
<td>- Enable SASL with MD5 Digest authentication?</td>
</tr>
<tr>
<td>VCS bind username</td>
<td>- username for the VCS login account; the sAMAccountName; Security Access Manager Account Name (in AD the Account’s user logon name)</td>
</tr>
<tr>
<td>Base DN for accounts</td>
<td>- starting search location for user accounts, including all ou=,dc= fields</td>
</tr>
<tr>
<td>Base DN for groups</td>
<td>- starting search location for groups, including all ou=,dc= fields</td>
</tr>
</tbody>
</table>
Appendix 2 – IT requisition (for group configuration)

To: IT Department

Please create a group called ____________________________ in the user authentication server and assign the following users to this group:

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24.
25.
Appendix 3 – Active Directory structure

The diagram below shows an example Active Directory tree structure for corporation.int:

```
corporation.int
  └── useraccounts
        └── region1
            └── marketing
                └── j.smith
            └── sales
                └── p.brown
            └── it
                └── r.ladd
        └── region2
            └── systems
                └── vcs
                    └── vcs_user
                        └── vcs_admin_rw
                            └── vcs_admin_ro
                                └── vcs_auditor
                                    └── member1
                                        └── member2
                                            └── memberN
                                └── ou=useraccounts,dc=corporation,dc=int
                                    └── ou=groups,dc=corporation,dc=int
```

Part of the VCS configuration required for connecting to an LDAP server includes the specification of a set of distinguished names (DNs). DNs comprise the following elements:
- **cn** common name (leaves of the tree – usually, see Note below)
- **ou** organizational unit (branches)
- **dc** domain content (top of tree)

These elements are listed in a single line as comma separated values. No space should be placed immediately before or immediately after the comma, but spaces are valid within the common names, organizational unit names and domain content names.

Using this example Active Directory structure you would define the **VCS bind DN** as:
```
cn=vcs,ou=systems,ou=region1,ou=useraccounts,dc=corporation,dc=int
```

To support **region 1** staff, the **Base DN for accounts** would be:
```
ou=region1,ou=useraccounts,dc=corporation,dc=int
```

To support **worldwide** staff, the **Base DN for accounts** would be:
```
ou=useraccounts,dc=corporation,dc=int
```

The **Base DN for groups** would be:
```
ou=groups,dc=corporation,dc=int
```
Note:

- Depending on how the database was initially set up, sometimes \texttt{cn=} is not reserved just for the 'leaves'. For example, by default Microsoft AD databases have the Users in a ‘container’ (\texttt{cn=}) not and organizational unit (\texttt{ou=}).
  When configuring the VCS bind DN and Base DN fields in VCS, it is important to use the same \texttt{dc, ou, cn} tags and use them in the same order as specified in the database.

- The VCS Bind DN is the directory structure to and including the object that specifies the account (in AD terminology the Active Directory “user” object). The account name used to login to the VCS and the account name used for SASL is the \texttt{sAMAccountName}; Security Access Manager Account Name (in AD the account’s user logon name).

- The Base DN for accounts and groups must be at or below the dc level (include all \texttt{dc=} values and maybe \texttt{ou=} values too). Having a base DN of \texttt{dc=int} is not supported.
Appendix 4 – Configuring groups in Active Directory

To allocate users to groups in Active Directory it is necessary to create a Group object and then make the user a member of that group.

Create a group object

1. From the Start menu, select Active Directory Users and Computers.
2. In the left hand folder display, choose the relevant folder in which to make the new group.
3. Ensure that no entry is selected in the right hand panel, then go to Action > New > Group.

4. Configure the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>The name for read write account access to VCS, for example VCS_admin_RW</td>
</tr>
<tr>
<td>Group scope</td>
<td>As required, for example Global</td>
</tr>
<tr>
<td>Group type</td>
<td>As required, for example Distribution</td>
</tr>
</tbody>
</table>

5. Create a second group for read-only access (for example, Group name = VCS_admin_RO).
6. Create a third group for auditor access (for example, Group name = VCS_auditor).
7. Create a fourth group for user access (for example, Group name = VCS_User).
Make a user a member of a group

1. From the Start menu, select Active Directory Users and Computers.
2. In the left hand folder display choose the relevant folder which holds the users.
3. Double-click on the required user.
4. Select the Member Of tab.

5. Click Add.

6. Enter part or all of the group name to which this user is to become a member.
7. Click Check Names.
8. Select the desired entry from the one or more group names presented.
9. Click OK to confirm the group.
10. Click OK to close the user properties dialog.

To allocate multiple users to a group in one go, select the users (hold Ctrl and click on each user), then right-click and select Add to a group... then continue at step 6 above.
Appendix 5 – Troubleshooting

Viewing / searching LDAP database

Windows

LDAP database viewers, such as the graphical “Softerra LDAP Administrator” package, let you look at the LDAP database contents.

Using the login credentials provided for the VCS, the LDAP viewer allows you to browse around to find users and groups.

You can check that users and groups are in appropriate paths by selecting the user or group and looking at its DN (distinguished name): the DN of a user should be a superset of the Base DN for accounts; the DN of a group should be a superset of the Base DN for groups.

Unix / Linux

ldapsearch (a program that is part of the openldap suite) can be used to query ldap databases, e.g.

```
ldapsearch -v -x -W -D "cn=vcs,ou=systems,ou=region1,ou=useraccounts,dc=corporation,dc=int" -b cn=p.brown,ou=it,ou=region1,ou=useraccounts,dc=corporation,dc=int -h server.corporation.int
```

will bind to the ldap server "server.corporation.int" as "vcs" and returns the directory information stored for the "p.brown" account (which would show information such as group membership).

For more information on ldapsearch, on a system supporting ldapsearch type:

```
man ldapsearch
```

Unable to log in after switching to remote authentication

Even when remote authentication is selected, the admin login remains accessible using the password configured on VCS.

Check that the LDAP and group settings on the VCS are correct. In particular, check for typing mistakes and use of spaces – spaces are allowed in group names.

AD “Domain Users” group fails to allow login

Default Active Directory groups such as the “Domain Users” group are seen as empty groups over LDAP and so should not be used as groups to define access rights. If they are selected, VCS will treat them as groups with no users.

Although when browsing in AD the “Domain Users” group is seen to have members (automatically added), when an LDAP search is performed on it, no member list is provided. VCS uses the LDAP member list to identify whether a user is a member of the group, and therefore whether that user should have the access rights of that group.

If a group does not provide access to the expected group of users, use an LDAP browser and check that there is a member list and that it contains the expected users.
Appendix 6 – Certificates for TLS

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

Note that the server address entered on the Login account LDAP configuration page on the VCS must match the CN (common name) contained within the certificate presented by the LDAP server.
Appendix 7 – Use with VCS clusters

All LDAP configuration is replicated across cluster peers, however the DNS server is configurable independently on each VCS peer. Make sure each peer references a DNS server that can lookup the LDAP server and (if SASL is enabled) can perform a reverse lookup of the LDAP server IP address.
Document revision history

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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>December 2009</td>
<td>Initial release.</td>
</tr>
<tr>
<td>2</td>
<td>March 2010</td>
<td>Updated for VCS X5.1.</td>
</tr>
<tr>
<td>3</td>
<td>October 2010</td>
<td>New document styles applied.</td>
</tr>
<tr>
<td>4</td>
<td>February 2011</td>
<td>Updated for VCS X6.</td>
</tr>
<tr>
<td>5</td>
<td>August 2012</td>
<td>Updated for changes to how administrator and user groups are configured in VCS X7.2.</td>
</tr>
</tbody>
</table>