



Authenticating Cisco VCS Accounts Using LDAP

Deployment Guide

First Published: December 2009

Last Updated: November 2015

Cisco VCS X8.7

Introduction

This document describes how to configure the Cisco TelePresence Video Communication Server (VCS) to authenticate and authorize login accounts over a centrally managed LDAP-accessible server.

LDAP authentication and authorization can be used for web login to the VCS's administrator and user (FindMe) accounts. Instead of looking up the username and password in its own internal database, the VCS contacts the LDAP accessible server to both authenticate the user and also to check whether that authenticated user belongs to a group that is authorized to access the VCS.

Using a central login credential database allows an enterprise 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.

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

Note that:

- Other logins, including serial and SSH continue to use the admin account configured on the VCS.
- User account web login only applies if you are using FindMe without Cisco TMS.

Process Summary

As an administrator 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 will be authenticated using credentials stored on the LDAP server.

Both the username and password are case sensitive.

LDAP Accessible Authentication Server Configuration

Define Groups in the Authentication Server

Defining groups in the authentication server is usually carried out by the IT department; use copies of the example requisition form (see [IT Requisition for Access to Authentication Server, page 13](#)) 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 exp_admin_rw)
- Read-only administrator (for example, group exp_admin_ro)
- Auditor administrator (for example, group exp_auditor)
- VCS user (for example, group exp_user)

VCS Configuration

Configure DNS Server

Ensure one or more DNS server addresses are set up on the VCS (**System > DNS**). 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. If SASL is enabled, the DNS servers must support reverse DNS lookup.

Configure LDAP Server Details on VCS

1. Go to **Users > 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 to get the appropriate information from your IT department):

Field	Description	Usage tips
Administrator authentication source	Select <i>Both</i> .	<i>Both</i> allows you to continue to use locally-defined accounts. This is useful while troubleshooting any connection or authorization issues with the LDAP server. You cannot log in using a locally-configured administrator account, including the default admin account, if <i>Remote only</i> authentication is in use. Note: do not use <i>Remote only</i> if VCS is managed by Cisco TMS.
FindMe authentication source	Select <i>Remote</i> .	This option applies only if you are using FindMe without Cisco TMS.

Field	Description	Usage tips
FQDN address resolution	<p>Defines how the LDAP server address is resolved.</p> <p><i>SRV record:</i> DNS SRV record lookup.</p> <p><i>Address record:</i> DNS A or AAAA record lookup.</p> <p><i>IP address:</i> entered directly as an IP address.</p> <p>Note: if you use SRV records, ensure that the records use the standard ports for LDAP. <code>_ldap._tcp.<domain></code> must use 389 and <code>_ldaps._tcp.<domain></code> must use 636. The VCS does not support other port numbers for LDAP.</p>	<p>The SRV lookup is for either <code>_ldap._tcp</code> or <code>_ldaps._tcp</code> records, depending on whether Encryption is enabled. If multiple servers are returned, the priority and weight of each SRV record determines the order in which the servers are used.</p>
Host name and Domain or Server address	<p>The way in which the server address is specified depends on the FQDN address resolution setting:</p> <p><i>SRV record:</i> only the Domain portion of the server address is required.</p> <p><i>Address record:</i> enter the Host name and Domain. These are then combined to provide the full server address for the DNS address record lookup.</p> <p><i>IP address:</i> the Server address is entered directly as an IP address.</p>	<p>If using TLS, the address entered here must match the CN (common name) contained within the certificate presented by the LDAP server.</p>
Port	<p>The IP port to use on the LDAP server.</p>	<p>Non-secure connections use 389 and secure connections use 636.</p>
Encryption	<p>Determines whether the connection to the LDAP server is encrypted using Transport Layer Security (TLS).</p> <p><i>TLS:</i> uses TLS encryption for the connection to the LDAP server.</p> <p><i>Off:</i> no encryption is used.</p>	<p>When TLS is enabled, the LDAP server's certificate must be signed by an authority within the VCS's trusted CA certificates file.</p> <p>Click Upload a CA certificate file for TLS (in the Related tasks section) to go to the Trusted CA certificate page.</p>
Certificate revocation list (CRL) checking	<p>Specifies whether certificate revocation lists (CRLs) are checked when forming a TLS connection with the LDAP server.</p> <p><i>None:</i> no CRL checking is performed.</p> <p><i>Peer:</i> only the CRL associated with the CA that issued the LDAP server's certificate is checked.</p> <p><i>All:</i> all CRLs in the trusted certificate chain of the CA that issued the LDAP server's certificate are checked.</p>	<p>If you are using revocation lists, any required CRL data must also be included within the CA certificate file.</p>

Field	Description	Usage tips
Bind DN	The distinguished name (case insensitive) used by the VCS when binding to the LDAP server. It is important to specify the DN in the order cn=, then ou=, then dc=	Any special characters within a name must be escaped with a backslash as per the LDAP standard (<i>RFC 4514</i>). Do not escape the separator character between names. The bind account is usually a read-only account with no special privileges.
Bind password	The password (case sensitive) used by the VCS when binding to the LDAP server.	The maximum plaintext length is 60 characters, which is then encrypted.
SASL	The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. <i>None</i> : no mechanism is used. <i>DIGEST-MD5</i> : the DIGEST-MD5 mechanism is used.	Enable Simple Authentication and Security Layer if it is company policy to do so.
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	The ou= and dc= definition of the Distinguished Name where a search for user accounts should start in the database structure (case insensitive). It is important to specify the DN in the order ou=, then dc=	This is for authentication of both administrator login and user login requests. 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.
Base DN for groups	The ou= and dc= definition of the Distinguished Name where a search for groups should start in the database structure (case insensitive). It is important to specify the DN in the order ou=, then dc=	This is for authorization of an authenticated user to log in as an administrator or to log in to a user account. If no Base DN for groups is specified, then the Base DN for accounts will be used for both groups and accounts.

3. Click **Save**.

For example, using the values from [Appendix 3: Example Active Directory Structure, page 15](#):

LDAP configuration You are here: [Users](#) > LDAP configuration

Remote account authentication

Administrator authentication source: ⓘ

User authentication source: ⓘ

LDAP server configuration

FQDN address resolution: ⓘ

Host name and Domain: . ⓘ

Port: * ⓘ

Encryption: ⓘ

Certificate revocation list (CRL) checking: ⓘ

Authentication configuration

Bind DN: * ⓘ

Bind password: ⓘ

SASL: ⓘ

Bind username: ⓘ

Directory configuration

Base DN for accounts: * ⓘ

Base DN for groups: ⓘ

Connection Status

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

State = Active

No error messages are displayed.

State = Failed

The following error messages may be displayed:

Error message	Reason / resolution
DNS unable to do reverse lookup	Reverse DNS lookup is required for SASL authentication.
DNS unable to resolve LDAP server address	Check that a valid DNS server is configured, and check the spelling of the LDAP server address.
Failed to connect to LDAP server. Check server address and port	Check that the LDAP server details are correct.
Failed to setup TLS connection. Check your CA certificate	CA certificate, private key and server certificate are required for TLS.

Error message	Reason / resolution
Failure connecting to server. Returned code<return code>	Other non-specific problem.
Invalid Base DN for accounts	Check Base DN for accounts ; the current value does not describe a valid part of the LDAP directory.
Invalid server name or DNS failure	DNS resolution of the LDAP server name is failing.
Invalid bind credentials	Check Bind DN and Bind password , this error can also be displayed if SASL is set to <i>DIGEST-MD5</i> when it should be set to <i>None</i> .
Invalid bind DN	Check Bind DN ; the current value does not describe a valid account in the LDAP director. This failed state may be wrongly reported if the Bind DN is 74 or more characters in length. To check whether there is a real failure or not, set up an administrator 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 Bind DN is wrong, the group is wrong or one of the other configuration items may be wrong.
There is no CA certificate installed	CA certificate, private key and server certificate are required for TLS.
Unable to get configuration	LDAP server information may be missing or incorrect.

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 **Users > Administrator groups**.
2. Click **New**.

3. Configure the fields as follows:

Name	Enter the group name to be used for the type of account required, for example: exp_admin_rw - for writeable access exp_admin_ro - for read-only access exp_auditor - for auditor access Note: the group name entered here must EXACTLY match (case sensitive) the group name entered in the AD or other authentication server.
Access level	Select the appropriate entry: <i>Read-write</i> : if writeable access is required. <i>Read-only</i> : if read-only access is required. <i>Auditor</i> : if access only to the Overview page and Log pages is to be allowed.
Web access	Select <i>Yes</i> .
API access	This controls access to the XML and REST APIs by systems such as Cisco TMS. Select <i>Yes</i> if members of this group need to access the system's APIs.
State	Select <i>Enabled</i> .

4. Click **Save**.

Administrator groups You are here: [Users](#) > Administrator groups

Configuration

Name	★ exp_admin_rw i
Access level	Read-write i
Web access	Yes i
API access	Yes i
State	Enabled i

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

User account web login only applies if you are using FindMe without Cisco TMS.

1. Go to **Users > FindMe groups**.
2. Click **New**.
3. Configure the fields as follows:

Name	Enter the group name to be used for a read/write account, e.g. exp_user Note: the group name entered here must EXACTLY match (case sensitive) the group name entered in the AD or other authentication server.
State	Select <i>Enabled</i> .

4. Click **Save**.

FindMe groups
You are here: [Users](#) > FindMe groups

Configuration

Name ★ exp_user (i)

State Enabled ▾ (i)

Save
Cancel

A warning is displayed at the top of the **FindMe 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).

Appendix 1: 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, for example

```
ldapsearch -v -x -W -D "cn=exp,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 "exp" 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 treats 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 2: Additional Information

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 **LDAP configuration** page on the VCS must match the CN (common name) contained within the certificate presented by the LDAP server.

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.

IT Requisition for Access to Authentication Server

To: IT Department

Please supply the following details so that the 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

LDAP server's Fully Qualified Domain or IP address	
If FQDN is it an A / AAAA record or SRV record?	A or AAAA / SRV
Port: IP port for the LDAP server (typically 389 or 636)	
Encryption: use TLS encryption to access the LDAP server? Certificate location?	YES / NO Path to certificate file:
Certificate revocation list	No checking / check single CA / check all CAs in trust chain
VCS bind DN: location of the VCS account object, including all cn=,ou=,dc= fields	
VCS bind password for the VCS login account	
SASL: enable SASL with MD5 Digest authentication?	YES / NO
VCS bind username: the username for the VCS login account; the sAMAccountName; Security Access Manager Account Name (in AD the Account's user logon name)	
Base DN for accounts: starting search location for user accounts, including all ou=,dc= fields	
Base DN for groups: starting search location for groups, including all ou=,dc= fields	

IT Requisition for Group Configuration

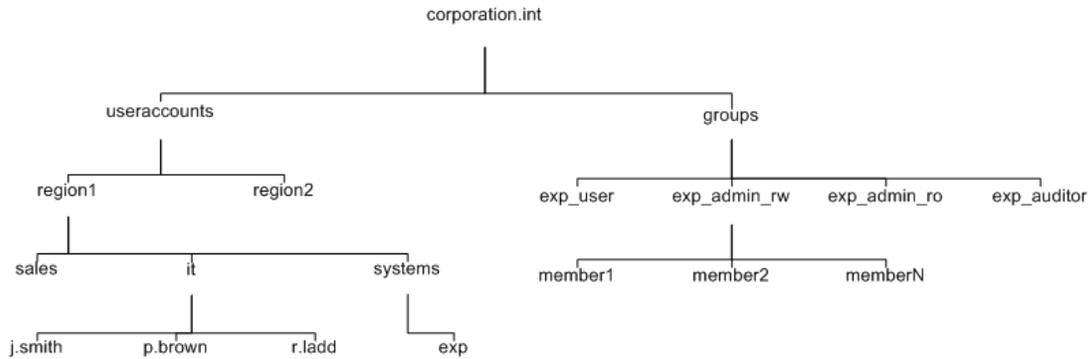
To: IT Department

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: Example Active Directory Structure

The diagram below shows an example Active Directory tree structure for corporation.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 cn= is not reserved just for the 'leaves'. For example, by default Microsoft AD databases have the Users in a 'container' (cn=) not and organizational unit (ou=).
When configuring the VCS **Bind DN** and **Base DN** fields in VCS, it is important to use the same 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 sAMAccountName; Security Access Manager Account Name (in AD the account's user logon name).
- The **Base DN for accounts** and **Base DN for groups** must be at or below the dc level (include all dc= values and maybe ou= values too). Having a base DN of dc=int is not supported.

Appendix 4: Configuring Groups in Active Directory

To allocate users to groups in Active Directory, you must 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:

Group name	The name for read-write account access to VCS, for example exp_admin_rw
Group scope	As required, for example Global
Group type	As required, for example Distribution

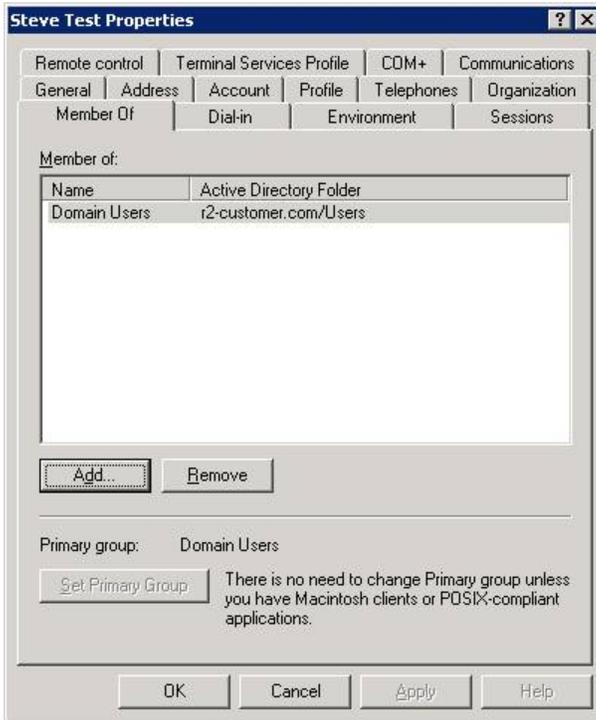
5. Create a second group for read-only access (for example, **Group name** = exp_admin_ro).
6. Create a third group for auditor access (for example, **Group name** = exp_auditor).
7. Create a fourth group for user access (for example, **Group name** = exp_user).



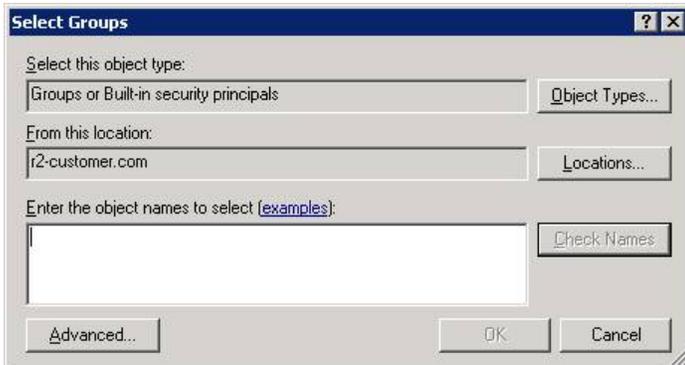
Make a User a Member of a Group

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.

Document Revision History

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

Date	Description
November 2015	New template applied. Republished for X8.7.
December 2014	Republished for X8.5.
June 2014	Republished for X8.2.
December 2013	Updated for VCS X8.1.
August 2012	Updated for changes to how administrator and user groups are configured in Cisco VCS X7.2.
February 2011	Updated for Cisco VCS X6.
October 2010	New document styles applied.
March 2010	Updated for Cisco VCS X5.1.
December 2009	Initial release.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2015 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)