Software Advisory: Secure LDAP Mandatory for Active Directory Connections

Revised: February 14, 2020

Software Advisory: Secure LDAP Mandatory for Active Directory Connections

This advisory covers all LDAP connections to Active Directory from the following Cisco Collaboration applications:

- Cisco Unified Communications Manager
- IM and Presence Service
- Cisco Unity Connection
- Cisco Expressway
- Cisco Meeting Server
- Cisco Meeting Management
- Cisco Jabber
- Cisco Unified Intelligence Center
- Cisco Unified Attendant Console Advanced

What's Changing

Microsoft is currently updating security requirements for LDAP connections to Active Directory. After this update completes, Secure LDAP (LDAPS) will become mandatory for all LDAP connections to Active Directory from the specified Cisco Collaboration applications. After the update, LDAP connections to Active Directory from these applications will not work unless Secure LDAP is configured.

This security update is not expected to become mandatory until the second half of the calendar year 2020. However, it's recommended that you update the specified Cisco Collaboration applications to use Secure LDAP as soon as possible. This will both secure your LDAP connection and will also ensure that services remain up and running when the security update becomes mandatory.

Why this Change is Needed

The existing default settings have a vulnerability that may expose Active Directory domain controllers to an elevation of privileges, and man-in-the-middle attacks. The Secure LDAP updates harden the connection to Active Directory's existing LDAP channel binding and LDAP signing mechanisms, making the system more secure. For more detailed information, refer to the Microsoft Security Advisory ADV190023:

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023

What configuration updates are required for Active Directory?

Microsoft is expected to roll out a security patch that updates Active Directory servers automatically once the patch is installed. Make sure to apply security patches promptly to Active Directory servers.

Prior to the security patch, administrators can edit Active Directory settings manually to secure the LDAP channel binding and LDAP signing mechanisms. The following three Active Directory registry settings must be changed from the current default setting of 0 to a new setting of 2. This will happen automatically when the patch is rolled out, but in the meantime, you must edit these manually:

- `ldapenforcechannelbinding`
- `ldapserverintegrity`
- `ldapclientintegrity`

For additional configurations around LDAP signing, see https://support.microsoft.com/en-us/help/935834.

What configuration updates are required for Cisco Collaboration Applications?

Before the requirements become mandatory, administrators must update any existing LDAP configurations that are non-secure for the specified Cisco Collaboration applications so that secure LDAP (LDAPS) is configured. If you already have LDAPS configured for all connections to Active Directory, no additional configuration updates are required.

Refer to the below sections for procedures on how to secure existing LDAP connections that are non-secure. Note that each of these updates should be applied only where Active Directory is used as the LDAP server, and the current connection is non-secure. The updates do not apply to other LDAP servers. Complete each update that applies to your deployment.

Note As part of the TLS confiiguration, you must also make sure that the appropriate LDAP trust certificates loaded onto each Cisco Collaboration application.

Cisco Unified Communications Manager Updates

For each LDAP directory sync:

1. From Cisco Unified CM Administration, go to **System** > **LDAP** > **LDAP Directory**.
2. Under **LDAP Server Information**, do the following for each LDAP server:
   - Make sure that the **LDAP Port** is set to the secure port of **636** or **3269**.
   - Check the **Use TLS** check box.
3. Click **Save**.

Note

- Make sure that you upload the appropriate certificates to the tomcat-trust store on Unified Communications Manager. The connection will work if you upload the LDAP server certificate or if you upload the root and/or applicable intermediate certificates of the certificate authority (CA) that signs the LDAP server certificate.
- The changes will not be implemented until the next LDAP sync occurs.

If you are using LDAP Authentication:

1. From Cisco Unified CM Administration, go to **System** > **LDAP** > **LDAP Authentication**.

2. Set the **LDAP Port** to the secure port of **636** or **3269**.
3. Check the **Use TLS** check box.
4. Click **Save**.

If you have LDAP Search configured, or Service Profile configured with Directory Profile, edit the UC service that points to Active Directory:

1. From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **UC Service**.
2. Click **Find** and select an existing directory service that points to Active Directory.
3. Set the **Port** to **636** or **3269**.
4. Set the **Protocol** to **TLS**.
5. Click **Save**.
6. Repeat this procedure for each UC Service that points to Active Directory.

IM and Presence Service Updates

If you are using XMPP contact search through a third-party LDAP server:

1. From Cisco Unified CM IM and Presence Administration, choose **Application** > **Third-Party Clients** > **Third-Party LDAP Servers**.
2. Click **Find** and select any Active Directory LDAP Servers.
3. Check the **Enable SSL** check box.
4. Click **Save**.
5. Repeat this process for each Active Directory LDAP Server.

For Centralized Deployments of the IM and Presence Service where you are syncing users from Active Directory, you must also apply the Unified Communications Manager secure LDAP configuration updates in the preceding section to the standalone Unified Communications Manager publisher node that is a part of the IM and Presence central cluster.

Cisco Unity Connection Updates

For Cisco Unity Connection LDAP syncs:

1. From Cisco Unity Connection Administration, choose: **LDAP** > **LDAP Directory**.
2. Under **LDAP Server Information**, set the following for any Active Directory connections:
    - Make sure that the **LDAP Port** is set to the secure port of **636** or **3269**.
    - Check the **Use TLS** check box.
3. Click **Save**.

If you are using an LDAP directory to authenticate Unity Connections users:

1. From Cisco Unity Connection Administration, choose: **LDAP** > **LDAP Authentication**.
2. Set the **LDAP Port** is set to a secure port of **636** or **3269**.

3. Check the **Use TLS** check box.
4. Click **Save**.

If you have Unity Connection Unified Messaging deployed with the Exchange Server Search option:

1. From Cisco Unity Connection, choose **Unified Messaging** > **Unified Messaging Services**.
2. Under **Exchange Servers**, set the **Protocol Used to Communicate with Domain Controllers** drop-down list box to **Secure LDAP (LDAPS)**.
3. Check the **Validate Certificates for Exchange Servers** check box.
4. Click **Save**.

Cisco Expressway Updates

Edit the following LDAP settings on Expressway-C for Active Directory connections:

1. Choose **Users** > **LDAP Configuration**.
2. Set the **Port** to **636**.
3. Set **Encryption** to **TLS**.
4. Click **Save**.

Cisco Meeting Server Updates

If you are using Cisco Meeting Server, edit your LDAP configuration for Active Directory:

1. From the Cisco Meeting Server administration interface, choose **Configuration** > **Active Directory**.
2. Set the **Port** to **636** or **3269**.
3. Check the **Secure connection** check box.
4. Click **Submit**.
5. Use SFTP to upload the certificate bundle of the LDAP server to the Cisco Meeting Server, and then run the following MMP commands:
   a. Run the `tls ldap trust <certificate_bundle>` command to assign the LDAP certificate.
   b. Run the `tls ldap verify enable` command to enable certificate verification.

Cisco Meeting Management

If you are using Cisco Meeting Management with Active Directory, follow these steps to reconfigure the system to use secure LDAP (LDAPS).

1. From the **Users** page, select **LDAP server**.
2. Check the **Use LDAP** check box.
3. For the **Protocol**, select the **LDAPS** radio button.
4. For the **Port**, enter **636** or **3269**.

5. Under **Certificate**, click the **Upload the certificate for your LDAP server** button.
6. Upload the LDAP certificate.
7. Save and Restart Meeting Management.

Cisco Unified Intelligence Center Updates

For Cisco Unified Contact Center Enterprise deployments, you must update the existing Active Directory configuration in Cisco Unified Intelligence Center:

1. From Cisco Unified Intelligence Center, choose **Cluster Configuration** > **Reporting Configuration** and select the **Active Directory** tab.
2. Set the port to a secure port: 686 or 3269.
3. Check the **Use SSL** check box.
4. Click **Save**.
5. After saving the configuration, upload the LDAP server certificate:
   a. Save the Active Directory certificate in Base-64 encoded X.509 (CER) file format.
   b. In Cisco Unified OS Administration, upload the certificate. Name the certificate as **tomcat-trust**.
   c. Run the `utils service restart Cisco Tomcat` CLI command followed by the `utils service restart Intelligence Center Reporting Service` command.

Cisco Unified Attendant Console Advanced Updates

Pre-existing Cisco Unified Attendant Console Advanced installations, whose LDAP directory sync is tied to Active Directory (AD) or Active Directory Lightweight Directory Services (ADLDS) also require the following configuration modifications (the following changes are not service impacting) where LDAPS is not already configured:

1. Install the required certificate(s) on the Cisco Unified Attendant Console Advanced server. This is only required on the Primary/Publisher server.
2. Login to the primary Cisco Unified Attendant Console Advanced web administration (`https://<hostname or IP address>/webadmin/login.aspx`).
3. Navigate to **System Configuration** > **Directory Source Management**.
4. Click **Select** beside the directory source that is being used: Microsoft Active Directory or Active Directory Lightweight Directory Services.
5. Modify the **Host Name or IP** value (if required).
6. Set the **Host Port** to reflect either 636 or 3269 (based on the requirements of your directory source).
7. Enable **Use SSL**.
8. Click **Save** and then **Test Connection** to validate the connection details.
9. Navigate to **Engineering** > **System Management**.
10. Stop and Start the Cisco Unified Attendant LDAP Plug-in.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.