Troubleshoot Directory Connector Authentication Failure with Account Mismatch on Windows Server

Contents

Issue

The Cisco Directory Connector installed on a Windows Server fails authentication when attempting to log in with a different admin account than the one used to sign into the server. The authentication process incorrectly attempts to use the Windows server login account instead of the intended Webex Control Hub admin account, resulting in these error messages:

- Authentication Failed
- Your account is not authorized. Please contact your administrator.

Backend logs show a SAML2 mapping error:

```
com.sun.identity.saml2.common.SAML2UserNotFoundException: No local user being mapped.
```

The Directory Connector previously prompted for account selection during log in, but after the issue onset, this prompt fails and authentication attempts are made with the incorrect account. Application reinstallation, service restarts, and server reboots do not resolve the initial authentication failure.

Environment

- Cisco Directory Connector installed on Windows Server 2019 Standard
- Server hosted on Google Compute Engine VM
- Server dedicated to Directory Connector with no other major services
- Separate user accounts in Active Directory: server admin account without email privileges and regular email account without server login privileges
- Directory Connector synchronization schedule configured with incremental sync timing
- BIOS mode set to Legacy with Secure Boot unsupported

Resolution

The authentication issue was resolved through these steps:

Step 1: Service Account Configuration

Change the Directory Connector service account to use a domain account with appropriate Active Directory privileges:

1. Open **services.msc** on the Windows Server.
2. Locate the **Directory Connector service**.
3. Change the running account from **Local System** to a **domain account** with sufficient AD privileges.
4. Restart the **Directory Connector service**.

Step 2: Account Mapping Verification

Ensure the Directory Connector's local log in matches the admin account in Webex Control Hub:

1. Verify that the email account used for Directory Connector has read permissions for AD user objects.
2. Confirm the account has privileges to connect to the Domain Controller and read Active Directory user objects.
3. If necessary, add the admin account as an alternate email in Active Directory per the deployment guide.

Step 3: Remove Redundant Instances

Remove any unneeded Directory Connector instances:

1. Navigate to the **Directory Connector interface**.
2. Click the **three dots** menu for the unneeded instance.
3. Select **Deactivate instance**.

Step 4: Sync Schedule Adjustment

Adjust the incremental sync timing from the default 24-hour interval to a preferred shorter interval as needed for the environment.

Step 5: Configuration Review

Review and confirm the Directory Connector configuration and synchronization schedule settings to ensure proper operation.

Cause

The primary root cause was a mismatch between the local server log in account and the Directory Connector/Webex admin account. The Directory Connector attempted to authenticate using the Windows server log in account instead of the intended Webex Control Hub admin account. This mapping failure occurred due to account separation in Active Directory, where the Directory Connector was unable to correctly map the Webex admin account when logged into the server with a different admin account. The SAML2 authentication process failed because no local user mapping could be established between the server log in account and the Webex Control Hub admin account.

Related Content

- Webex Directory Connector Deployment Guide
- Cisco Technical Support & Downloads