Cisco Directory Connector Guide for Administrators

📄 Document created by **Cisco Documentation Team** on Nov 9, 2016 • Last modified by **Cisco Documentation Team** on Jun 23, 2017

☰ **Version 23**

👍 Like • 0   💬 Comment • 0   ⤢

Directory Connector

Directory Connector is the client software that is installed on your local machine. It connects and

communicates with the connector service. Directory Connector is the on-premises application for identity synchronization in to the cloud.

With Directory Connector, you can maintain your user accounts in the Active Directory single source and do the following:

- Synchronize identities, users, and groups, from your Active Directory to the cloud and create Cisco Spark user accounts from the Active Directory Source. (The Directory Connector does not synchronize user passwords.)

- Automatically schedule when to perform a synchronization.

- Perform a dry run synchronization.

Directory Connector is divided into three areas:

- **Cisco Cloud Collaboration Management** is the single interface that lets you manage all aspects of your Cisco Spark organization: view users, assign licenses, download Directory Connector, and configure single sign-on (SSO) for users who want to authenticate through their enterprise identity provider.

- **Directory Connector management interface** is where you can run a synchronization, view and monitor synchronization status, and configure Directory Connector services.

- **Directory synchronization service** queries your Active Directory to retrieve users and groups to synchronize to the connector service and Directory Connector.

Related Information

Single Sign-On Integration Guides for Cisco Spark

Install Directory Connector

System Requirements for Directory Connector

You can install Directory Connector on these Windows Servers:

- Windows Server 2016

- Windows Server 2003

- Windows Server 2008 R2

- Windows Server 2012

Directory Connector works with Active Directory 2008, 2008 R2, 2012, and 2012 R2. In addition:

- You must have NET Framework v3.5 on the machine where Directory Connector is installed.

- If your machine has Windows 2003, make sure that you have .NET Framework v3.5.

- If your machine has Windows 2008 R2 or later, verify that v3.5 is preinstalled on it.

Minimum Requirements

Directory Connector requires a computer with

- 8 GB of RAM

- 50 GB of storage

- No minimum for the CPU

Prerequisites for Directory Connector

- We recommend that you install Directory Connector and Active Directory Domain Service/Active Directory Lightweight Directory Services (AD DS/AD LDS) on separate machines.

- The machine with Directory Connector installed needs an administrator account to authenticate the Directory Connector machine to the on-premises domain that has DNS enabled.

- If your network is behind a firewall, ensure that your system has HTTPS (port 443) access to the Internet.

Related Information

Manage Cisco Spark User Accounts

Install Directory Connector

Install the latest version of Directory Connector from Cisco Cloud Collaboration Management.

1   Sign in to https://admin.ciscospark.com with your administrator credentials.

2   Go to **Users**, click **Manage Users**, and then choose **Enable Directory Synchronization**.

3   Click the **Download and Install** link to save the installation .zip file to your VMware or Windows server.

4   On the VMware or Windows server, unzip and run the .msi file in the setup folder to launch the **Cisco Directory Connector Setup Wizard**.

5   Click **Next**.

6   Click **I Agree** to accept the license agreement, and then click **Next** until you see the account type screen.

7 Choose the type of service account that you want to use and perform the installation with an admin account:

- **Local System**—The default option. You can use this option if you have a proxy configured through Internet Explorer.
- **Domain Account**—Use this option if the computer is part of the domain. Directory Connector must interact with network services to access domain resources. You can enter the account information and click OK. When entering the **Username**, use the format {domain}\{user_name}

  Note   For a proxy that integrates with AD (NTLMv2 or Kerberos), you must use the domain account option. The account used to run Directory Connector Service must have enough privilege to pass proxy and access AD. The account must also have the local Administrator Role, because it must access access files under C:\Program Files.

8 Click **Next**.

After the Directory Connector is successfully installed, the **Installation Complete** screen appears.

9 Click **Finish**.

Sign In To Directory Connector

1 Sign in to the Directory Connector.

You may get a prompt to add https://idbroker.webex.com to your list of trusted sites.

2 After this prompt, **Sign in to Spark** using your admin account.

3 Confirm your organization and domain.

- If you choose **AD DS**, choose the domain that you want to synchronize to from, and then click **Confirm**.
- If you choose **AD LDS**, enter the host, domain, and port and then click the **Refresh** button to load all application partitions. Then select the partition from the drop-down list and click **Confirm**. See the AD LDS section for more information.

4 After the Directory Connector **Confirm Organization** screen appears, click **Confirm**.

If you already bound AD DS/AD LDS, the **Confirm Organization** screen appears.

5 Click **Confirm**.

6 Choose one, depending on the number of Active Directory domains you want to bind to Directory Connector:

- If you have a single domain that is **AD LDS**, bind to the existing AD LDS source, and

then click **Confirm**.

- If you have a single domain that is **AD DS**, bind to the existing domain or to a new domain. If you choose **Bind to a new domain**, click **Next**.
Because the existing source type is AD DS, you cannot select **AD LDS** for the new binding.

Related Concepts

AD LDS with Directory Connector

Directory Connector Dashboard

When you first sign in to Directory Connector, the Dashboard appears. Here you can view a summary of all synchronization activities, view cloud statistics, perform a dry run synchronization, start a full or incremental synchronization and launch the event view to see error information.

✎

Note

If your session times out, sign back in.

You can easily run these tasks from the Actions Toolbar or Actions Menu.

Table 1 **Dashboard Components**

Current Synchronization	Displays the status information about the synchronization that is currently underway. When no synchronization is being run, the status display is idle.
Next Synchronization	Displays the next scheduled full and incremental synchronizations. If no schedule is set, **Not Scheduled** is displayed.
Last Synchronization	Displays the status of the last two synchronizations performed.
Current Synchronization Status	Displays the overall status of the synchronization.

Connectors	Displays the current on-premises connectors that are available to the Cloud.
Cloud Statistics	Displays the overall status of the synchronization.
Synchronization Schedule	Displays the synchronization schedule for incremental and full synchronization.
Configuration Summary	Lists the settings that you changed in the configuration. For example, the summary might include the following: • All objects will be synchronized • All users will be synchronized • Deleted threshold has been disabled.

Table 2 **Actions Toolbar**

Start Incremental Sync	Manually start an incremental synchronization (disabled when you pause or disable synchronization, if a full synchronization was not completed, or if synchronization is in progress)
Sync Dry Run	Perform a dry run synchronization.
Launch Event Viewer	Launch the Microsoft Event Viewer.
Refresh	Refresh the Directory Connector dashboard

<p style="text-align:center">Table 3 Actions Menubar</p>

Sync Now	Start a full synchronization instantly.
Synchronization Mode	Select either incremental or full synchronization mode.
Reset Connector Secret	Establish a conversation between Directory Connector and the connector service. Selecting this action will reset the secret in the cloud and then saves the secret locally.
Dry Run	Perform a test of the synchronization process. You must do a dry run before you do a full synchronization.
Troubleshooting	Turn on/off troubleshooting.
Refresh	Refresh the Directory Connector main screen.
Exit	Exit Directory Connector.

<p style="text-align:center">Table 4 Key Combinations</p>

Key Combination	Action

Alt +A	Show the **Actions** menu
Alt +A + S	Synchronization now
Alt +A + R	Reset Connector Secret
Alt +A + D	Dry run
Alt +A + S + I	Incremental synchronization
Alt +A + S + F	Full synchronization
Alt + H	Show**Help**menu
Alt + H + H	Help
Alt + H + A	About
Alt + H + F	FAQ

Configure Directory Connector

Configure General Settings

You can configure the name of the server running Directory Connector, the log levels, and the preferred settings for the domain controllers. The name of the connector appears on the dashboard in the connectors section, along with any other connectors that are running.

1   From **Directory Connector**, click the **Configuration** tab.

2   Click the **General** tab.

3   In the **Connector Name** field, enter the connector name. This field shows only the computer name that is currently running the connector.

4   Choose the log level from the drop-down. By default, the log level is set to **info**. The available log levels are:

- Info

- Debug

- Warn

- Error

5   Choose the **Preferred Domain Controllers** to set the order of domain controllers for synchronizing identities.
The domain controllers are accessed from top to bottom. If the top controller is unavailable, choose the second controller on the list. If no controller is listed, you can access the primary controller.

Select the Connector Object

You can select an object and its container. By default, all users that are not computers, and all groups that are not critical system objects, are synchronized with the entire domain.

1   From **Cisco Directory Connector**, click **Configuration**, and then choose **Object Selection**.

2   In the **ObjectType** section, click either **Users** or **Groups**. Consider limiting the number of searchable containers for users and groups.

3   Configure the **LDAP** filters. You can add extended filters by providing a valid LDAP filter.

4   Specify the**On Premises Base DNs to Synchronize**.

To synchronize only the users that are enabled in Active Directory, add the domain names (DNs) without the quotes.

For example: (!(userAccountControl:1.2.840.113556.1.4.803:=2))

5   Click **Select** to see the tree structure of your Active Directory. From here, you can select or de-select which containers to search on.

6   Check that the objects you want to add for this configuration, and click **Select**.

You can select individual or parent containers to use for synchronization. Select a parent container to enable all child containers. If you select a child container, the parent container shows a gray check mark that indicates a child has been checked. You can then click **Select** to accept the Active Directory containers that you checked.

If your organization places all users and groups in the Users container, you do not have to search other containers. If your organization is divided into organization units, make sure that you select **OUs**.

7   Click **Apply**.

Choose an option:

- Apply Config Changes

- Dry Run

- Cancel

For information on dry runs, see "Perform A Dry Run Synchronization."

Related Tasks

Perform a Dry Run Synchronization

Configure the Connector Policy

You can set the maximum number of deletes that can occur during synchronization. Running

synchronization does not delete objects from your on-premises Active Directory. All objects are deleted only from the cloud.

For example, you set 1 as the delete threshold trigger value. When you do full or incremental sync, if the number of users you want to delete is more than the setting, the directory connector shows a warning. If you click **Override Threshold**, you can start full or incremental sync successfully, but you will see this override notice the next time you run the policy.

1   From **Directory Connector**, click **Configuration**, and then choose **Policy**.

2   Check the **Enable delete threshold trigger** box if you want to add a threshold trigger. Choosing this option triggers an alert if the number of deletes exceeds the threshold. When the deletion account exceeds the one that you define, the synchronization fails.

3   Enter the maximum number of deletes that you want. The default is 20.

    Note   We recommend that you do not increase the default value.

4   Click **Apply**.

Set the Connector Schedule

You can set the times that you want to synchronize your Active Directory. Failover is used for high availability (HA). If one connector is down, we switch to another standby connector after the predefined interval.

1   From Directory Connector, click **Configuration**, and then choose **Schedule**.

2   Specify the **Incremental Synchronization Interval** in minutes. By default, an incremental synchronization is set to occur every 10 minutes. The full incremental synchronization does not occur until you initially perform a full synchronization.

3   Change the **Send Reports per… time** value if you want the change how often reports are sent.

4   Check **Enable Full Sync Schedule** to specify the days and times on which you want a full synchronization to occur.

5   Specify the **Failover Interval** in minutes.

6   Click **Apply**.

Map User Attributes

You can map attributes from your local Active Directory to corresponding attributes in the cloud. The only

required field is the *uid.

Note

Accounts in Active Directory must have an email address; the uid maps by default to the ad field of mail (not sAMAccountName).

For detailed information on mapping options, see Mapping Active Directory Attributes in Directory Connector.

1   From **Directory Connector**, click **Configuration**, and then choose **User Attribute Mapping**.
    This page shows the attribute names for Active Directory and the Cisco cloud. All required attributes are marked with a red asterisk.

2   Choose the **Active Directory Attribute Names** that you want to map to the cloud. Next to each attribute name is a drop-down of attributes from which you can choose.

3   After you make your choices, click **Apply**.

Any user data that is contained in Active Directory overwrites the data in the cloud that corresponds to that user. For example, if you created a user manually in Cisco Cloud Collaboration Management, the user's email address must be identical to their email in Active Directory. Any user without a corresponding email address in AD is deleted.

Active Directory Attributes in Directory Connector

You can map attributes from your local Active Directory to corresponding attributes in the cloud by using the **User Attribute Mapping** tab.

This table describes the mapping between the Active Directory Attribute Names and the Cisco Cloud Attribute Names.

Active Directory Attribute Names	Cisco Cloud Attribute Names
buildingName	
c	c
departmentNumber	departmentNumber
displayName	displayName
userAccountControl	ds-pwp-account-disabled
employeeNumber	employeeNumber
employeeType	employeeType
facsimileTelephoneNumber	facsimileTelephoneNumber
givenName	givenName
	jabberID

l	l
	locale
manager	manager
mobile	mobile
msRTCSIP-PrimaryUserAddress	sipAddresses
o	o
*objectGUID	onPremObjectGUID
ou	ou
physicalDeliveryOfficeName	physicalDeliveryOfficeName
postalCode	postalCode
preferredLanguage	preferredLanguage
sn	sn

st	st
streetAddress	street
telephoneNumber	telephoneNumber
	timezone
title	title
type	enterprise
*mail	uid

Configure an Avatar

You can synchronize your users' avatars to the cloud so that each user's avatar appears when they sign in to the application.

Before You Begin

The URI pattern and variable value in this procedure are examples. You must use actual URLs where your directory avatars are located.

1   From the Directory Connector, go to **Configuration**, and then click **Avatar**.

2   Enter the **Avatar URI Pattern**—For example, **http://www.example.com/dir/photo/zoom/**
    🔗{mail: .*?(?=@.*)}.jpg
    The avatar URI pattern must be reachable from the internet.

3   Enter the **Variable Value**—For example: ✉ **abcd@example.com**.

4   Click **Test**.

Example:

In this example, if the mail value for one AD entry is ✉ **abcd@example.com**, the **Final Avatar URI** is **http://www.example.com/dir/photo/zoom/abcd.jpg** ⧉

5   After the URI information is verified, check **Enabled**, and then click **Apply**.

For detailed information about using regular expressions, see the Microsoft Regular Expression Language Quick Reference ⧉ .

Run Active Directory Synchronization

Perform a Dry Run Synchronization

When you perform a dry run, Directory Connector retrieves the information from your Active Directory, based on the configuration parameters that you set. This information is then compared against the information stored in the cloud. A dry run allows you to see what objects will be added, modified, or deleted when you run a full or incremental synchronization.

Cisco
directory connector

Summary | 0 Admins Deleted | 2 Users Deleted | 0 Groups Deleted | 2 Objects Added | 10 Objects Matched

Summary of Dry Run

TIP: Select corresponding tab to see list of affected object categories in details.

0   Admin objects will be deleted

2   Non Admin user objects will be deleted

0   Group objects will be deleted

2   Objects will be added

10   Objects Matched

Delete threshold (1 object) exceeded. 2 objects would be deleted

Save Results to File...   Done

Perform a dry run before you enable synchronization, or when you change the synchronization parameters. If the dry run was initiated by a configuration change, you can save the settings after the dry run is complete.

1   From **DirectoryConnector**, click **Dashboard**, and then choose **Sync Dry Run**.

2   Click **OK** to start a dry run synchronization.

- Email address is the key value for users. Users without email addresses who are in Active Directory are not listed in the dry run report.

- If a user in the cloud doesn't have a corresponding user with the same email in Active Directory, the entry is listed under **Admin objects will be deleted**. To avoid this delete flag, you can add a user in Active Directory with the same email address.

What to Do Next

To view the details of the items that were synchronized, click the corresponding tab for specific items or **Objects Matched**. To save the summary information, click **Save Results to File**.

Run a Full Synchronization

When you run a full synchronization, the connector service sends all filtered objects from your Active Directory (AD) to the cloud. The connector service then updates the identity store with your AD entries.

You can only run a full synchronization after you configure a full synchronization schedule.

Directory Connector synchronizes the user account state—In Active Directory, any users that are marked as disabled appear as disabled in the cloud, too.

1   From Directory Connector, go to the **Dashboard**, click **Actions**, and then choose
   Synchronization Mode > Enable Synchronization.
   When you enable synchronization, Directory Connector asks you to perform a dry run first.

2   Click **Sync Now > Full** to start the synchronization.

- During the synchronization, the dashboard shows the synchronization progress; this may include the type of synchronization, the time it started, and what phase in which the synchronization is currently running.

- After synchronization, the **LastSynchronization and Cloud Statistics** sections are updated with the new information.

If errors occur during the synchronization, the status indicator ball turns red.

For information about errors, select the **LaunchEvent Viewer** from the**Actions** toolbar to view the error logs.

Run an Incremental Synchronization

An incremental synchronization queries your Active Directory and looks for changes that occurred since the last synchronization. This step then bundles those changes and sends them to the connector service.

1 From Directory Connector, click **Dashboard**.

> **Note**
>
>> When you enable synchronization, Directory Connector asks you to perform a
>> dry run first.

2 From **Actions**, click **Synchronization Mode > Enable Synchronization**.

3 From **Actions**, click **Sync Now > Incremental**.

- During the synchronization, the dashboard shows the synchronization progress; this may include the type of synchronization, the time it started, and what phase in which the synchronization is currently running.

- After synchronization, the **LastSynchronization and Cloud Statistics** sections are updated with the new information.

If errors occur during the synchronization, the status indicator ball turns red.

For information about errors, click **LaunchEvent Viewer** from the**Actions** toolbar to view the error logs.

Related Tasks

Launch the Event Viewer

Launch the Event Viewer

To see the events that occurred during a full or incremental synchronization, launch the **Event Viewer**. It displays a summary of the administrative events and error logs

> **Note**
>
>> Event logs capture user actions. For help with managing network traffic, **Enable Troubleshooting**.

1   From Directory Connector, click the **Dashboard** tab.

2   Click **Launch Event Viewer** from the **Action** toolbar.

   The Event Properties dialog shows the synchronization event details and error details.

Manage Directory Connector

Enable Troubleshooting for Directory Connector

You can enable troubleshooting to help diagnose any errors you encounter in Directory Connector. Troubleshooting lets you capture the network traffic information and save it to a file.

Locate the troubleshooting file: <Installation Location>\Cisco Systems\Cisco Systems\Cisco Directory Connector\Data\Troubleshooting.txt

1   Run the services.msc file to change the running account for the Directory Connector service from the Local System to a domain account that has privileges to access your AD DS or AD LDS.

2   Restart the service.
   See How to Start Services ⧉ for guidance.

3   In Directory Connector, click **Dashboard**.

4   Go to **Actions**, and then click **Troubleshooting**.

5   With troubleshooting enabled, repeat the actions that were causing an error; this captures the traffic data so that it can be examined.

6   Examine the log file: if the file is blank, make sure that the account has privileges to access your AD DS or AD LDS.

7   If necessary, send the log file to support for assistance.

8   Disable the troubleshooting feature when you are done.

Related Information

📄 How to Contact Support

Upgrade Directory Connector

Directory Connector automatically notifies you when a new version is available. Always upgrade to the latest version to avoid problems. You also see a notification in the Windows task bar.

Before You Begin

Disable the existing synchronization.

1 From Directory Connector click **Dashboard**.

2 Go to **Actions**, click **Synchronization Mode** and then choose **Disable Synchronization**.

3 Either click on the notification, or right-click on the icon in the Task Bar to start the upgrade process.

4 Follow the instructions to complete the upgrade.

When the upgrade process is complete, be sure to verify the version number.

Uninstall and Deregister Directory Connectors

After you uninstall an instance of Directory Connector, you must deregister it. Completely remove a Directory Connector for any of these scenarios:

- You don't want to use directory synchronization any more.

- You don't want to use one of multiple directory connectors (high availability).

- You want to change the domain and install another connector.

Before You Begin

- You may have multiple instances of Cisco Directory Connectors set up for high availability (HA). Disable the synchronization if you are uninstalling the only or last remaining instance of Directory Connector.

- Save and close any important work before you uninstall the Directory Connector.

1 From your Windows machine, go to Control Panel, and then click **Programs and Features**.

2 From the program list, click **Cisco Directory Connector**, choose **Uninstall**, and then follow the prompts.
   You might have to reboot your system to complete the uninstallation.

3 Open a new browser tab and sign in to Cisco Cloud Collaboration Management with your administrator credentials.

4 Click **Settings**. From the Active Directory section, click **Deregister** next to the directory connector that you want to uninstall.

5 After you read the prompt, click **Deregister**.

Unless there's another Directory Connector in a high availability (HA) deployment, user accounts are not synchronized any more.

AD LDS and Directory Connector

AD LDS with Directory Connector

A data model restriction (a single LDAP partition view or a single organizational unit (OU) view) may be imposed on an enterprise directory-enabled application. This application must access data that is associated with AD DS-authenticated users, applications, or network resources that are located in multiple forests, domains, or OUs in the enterprise.

In this situation, AD LDS is used to synchronize its user database with different AD Domain Controllers or other LDAP sources. In such a case, choose Domain Account for AD LDS item when you install Directory Connector.

If your environment has multiple domains/forests, set up AD LDS and bind the Directory Connector to the parent domain. AD LDS provides Directory Connector with a consolidated view of multiple domains/forests.

About AD LDS

You can use Microsoft Active Directory Lightweight Directory Service (AD LDS), to provide directory services for directory-enabled applications. Rather than use your organization's Active Directory Domain Service (AD DS) database to store the directory-enabled application data, AD LDS can be used to store the data.

You can use AD LDS with AD DS so that you can have a central location for security accounts (AD DS) and a separate location to support the application configuration and directory data (AD LDS).

With AD LDS you can:

- Reduce the overhead associated with AD replication

- Avoid the need to extend the AD schema in order to support the application

- Partition the directory structure so that the AD LDS service is only deployed to the servers that need to support the directory-enabled application

See When Should I Use AD LDS Role? ⤢ to understand seven scenarios that require using AD LDS.

You can set up your AD LDS environment by following the AD LDS Getting Started Step-by-Step Guide ⤢.

Use AD LDS with Directory Connector

A limited set of server roles is available for the Server Core installation option of Windows Server 2008 and

for Windows Server 2008 for Itanium-Based systems.

Before You Begin

Review the Using AD LDS ⧉ documentation.

1 To install the AD LDS server role on a computer running Windows Server 2008, see Install the AD LDS Server Role ⧉.

2 To begin working with AD LDS instances, see Practice Working with AD LDS Instances ⧉.

3 To import data from a file into an AD LDS instance, see:Import data into an AD LDS instance ⧉.

4 To import from AD DS, see:Synchronize with AD DS ⧉.

5 If you set up multiple partitions in AD LDS, choose the one you need, and then click **Confirm** in the Directory Connector Confirm Organization window.

Web Proxy Integration

Directory Connector with Web Proxy Integration

If web proxy authentication is enabled in your environment, you can still use Directory Connector.

If your organization uses a transparent web proxy, it does not support authentication. Directory Connector successfully connects and synchronizes users.

You can take one of these approaches:

- Explicit web proxy through Internet Explorer (Directory Connector inherits web proxy settings)

- Explicit web proxy through a .pac file (Directory Connector inherits enterprise-specific proxy settings

- Transparent Proxy that works with Directory Connector without any changes

Use a Web Proxy Through The Browser

You can set up Directory Connector to use a web proxy through Internet Explorer.

If the Cisco DirSync Service runs from a different account than the currently signed in user, you also need to sign in with this account and configure web proxy.

1   From Internet Explorer, go to **Internet Options**, click **Connections**, and then choose **LAN Settings**.

2   Point the Windows instance where Directory Connector is installed at your web proxy. Directory Connector inherits these web proxy settings

3   If your environment uses proxy authentication, add cloudconnector.cisco.com to your allowed list for sites that have proxied authentication turned off. You may perform this either site-wide (for all hosts) or just for the host that is Directory Connector.

   Note

         If you add cloudconnector.cisco.com to an allowed list to completely bypass your web proxy, make sure your firewall ACL table is updated to permit the Directory Connector host to access cloudconnector.cisco.com directly.

Configure Web Proxy Through a PAC file

Your administrator can configure your client browser to use a .pac file which in turn supplies the web proxy address and port information. Directory Connector directly inherits the enterprise-specific web proxy configuration.

1   For Directory Connector to successfully connect and sync user information with Cisco Spark and WebEx, make sure proxy authentication is disabled for cloudconnector.cisco.com in the .pac file configuration for the host where Directory Connector is installed.

2   If you add cloudconnector.cisco.com to an allowed list in order to completely bypass your web proxy, make sure your firewall ACL table is updated to permit the Directory Connector host to access cloudconnector.cisco.com directly.

Configure Transparent Proxy

In this scenario, the browser is unaware that a transparent web proxy is intercepting http requests [80/443] and no client-side configuration is required.

When you deploy a transparent proxy, Directory Connector successfully connects and synchronizes users.

You can confirm that the proxy is successful if you see normal browser authentication popup window behavior when starting Directory Connector.

Disable Proxy Authentication

You can disable proxy authentication in your enterprise, if you are not using a proxy server to handle authentication requests.

Set Proxy Authentication for Directory Connector

Add the URL cloudconnector.cisco.com to your allowed list by creating an Access Control List. On your enterprise firewall server:

1   Enable DNS lookup if not already enabled.

2   Determine an estimated bandwidth for this connection (Directory Connector at ~2 mb/s or less). This may not be required.

3   Create an Access Control List to apply to the Directory Connector host, and specify cloudconnector.cisco.com as the target to add to the allowed list.
    For example:
      access-list 2000 acl-inside extended permit TCP [IP of the Directory Connector] cloudconnector.cisco.com eq https

4   Apply this ACL to the appropriate firewall interface, which is only applicable for this single host (Directory Connector).

5   Ensure that the rest of the hosts in your enterprise are still required to use your web proxy by configuring the appropriate implicit deny statement.

Troubleshoot Service Account Sign In Issues

If you can't sign in to Directory Connector or can't run a synchronization, use these steps to try to resolve the issue before contacting support.

1   Try to visit https://cloudconnector.cisco.com/SynchronizationService-v1_0/?orgId=GLOBAL ⧉ in your web browser.

2   Choose one, depending on the results:

    • If you can't visit the link from your browser, check your network settings. if your environment uses proxy, check the proxy settings.

- If you can visit the link from your browser but can't open Directory Connector (**Can't open connector and pop up error message with 407**), go to the customer view in https://admin.ciscospark.com and make sure you get the latest version of Directory Connector. You can contact the support team for help, too.

- If you can visit the link from your browser but can't run a synchronization from the Directory Connector, change the service login account for to **domain admin**.

Related Information

Contact support

Manage Cisco Spark User Accounts

Assign Cisco Spark Services to Your Directory Synchronized Users

After you complete user synchronization through Directory Connector, you can assign Cisco Spark service licenses to all of your users at once. You can make individual changes after this initial step.

1 From the customer management portal, go to users **Users**, and then click **Manage Users**.

2 Click **Advanced**, and then click through the prompts until you reach Sync Status.

3 Click the refresh arrow to reload the list.

4 Click **Next**.

5 Check the Cisco Spark services that you want to apply initially to all of the synchronized users.

- At this point, an email is sent to each user with an invite to join and download Cisco Spark.

- Users must accept the invitation to be added to your organization.

6 Change assigned services for users.

If you selected the same Cisco Spark services for all of your users, afterwards you can make changes individually or in bulk.

Related Information

Change services for individual users

Change services for users in bulk

User Is Notified When Assigned a License

When an administrator assigns a license to a user, the user receives an email confirming that the license

has been assigned.

The email is sent by Cisco Cloud Collaboration Management.

Change a Cisco Spark Email Address

If your organization does not use the Cisco Directory Connector, you can change your Cisco Spark email addresses through the account settings at https://idbroker.webex.com/idb/profile#/ ⧉

If you want to change your email addresses using the Cisco Directory Connector, you change those email addresses in Active Directory. After the next synchronization, the changes appear in Cisco Spark. There is no loss of data or spaces using this method. The on-premises user ID is set in the cloud after the first synchronization. All subsequent synchronizations are based on the user ID.

Change the Active Directory Domain

You can use this procedure to create new domains and email addresses that are synchronized with the identity service in the cloud.

1 Set up a new Active Directory (AD) domain.

2 Disable synchronizations on all of your Cisco Directory Connectors.

3 Uninstall all of your Cisco Directory Connectors.

4 Open a case to change the domain:
   https://support.ciscospark.com/customer/en_US/portal/emails/new ⧉.

5 After the case is resolved:

   1. Install the Cisco Directory Connector on the same server as the one with the new AD domain.

   2. Configure the Cisco Directory Connector so that its point to the new AD domain.
      If there are existing users in Cloud Collaboration Management (the management portal), ensure that users with matching email addresses are also present in AD. User email addresses that are in the management portal but not in AD are deleted from the portal.

   Perform a test run with the Cisco Directory Connector before doing the actual synchronization.

Domain Claim

A domain claim occurs if you claim an email domain for an organization so that any sideboarded account is

created in the customer organization and not the free consumer organization.

If the Cisco Directory Connector is active and the domain is claimed, sideboarded accounts are not created either in the customer organization or in the free consumer organization. Only the Cisco Directory Connector may provision accounts for the organization from Active Directory. The information stored on Active Directory is the original source. If you attempt to sideboard an account, the invited user receives an error. The only way that an invited user can be added to a Cisco Spark space is by using the Cisco Directory Connector to provision the account.

Convert Cisco Spark Users in a Directory Synchronized Organization

You can only use unique email addresses in the Cisco Spark directory. If your users have signed up for the free version of Cisco Spark, their account exists in the free consumer organization.

To manage users in this organization using Directory Connector, migrate (convert) them to the customer organization before you turn on the Directory Connector.

If you do not convert the accounts before activation, turn off the Directory Connector in order to convert them.

If you attempt to convert a user while directory synchronization is enabled, the error message "<email address> could not be converted" appears.

To avoid the problem, you can use this workaround.

Before You Begin

⚠️

Caution

If any converted users are deleted, they lose all their Cisco Spark spaces.

1   Disable the directory synchronization from the Directory Connector.

2   📄 Convert the user from the free consumer organization to the enterprise organization.

3   On the Directory Connector, run a dry run. When the dry run completes, check the Delete Users tab. Verify that any users that you converted are not deleted.

4   When you are sure that the next synchronization will not remove any accounts, reenable directory synchronization from the Directory Connector.

Sideboarded Cisco Spark User Accounts

When you invite another user to a space in Cisco Spark, if the invited user does not exist in the Cisco Spark directory, an account is created for them ("sideboarded"). By default, accounts that are created this way are added to the free consumer organization.

If you want to manage the sideboarded account using the Cisco Directory Connector, you must 🗎 convert the account.

Change Cisco Spark Username Format After Directory Synchronization

By default, Directory Connector maps the displayName attribute in Active Directory to the displayName attribute in the cloud.

After performing a directory synchronization, you may find that usernames display in the format <lastName, firstName>.

This username may appear if the "displayName" attribute in Active Directory is configured that way. When the attribute is mapped to "displayName" in the cloud, names show up in the format <lastName, firstName> in Cisco Cloud Collaboration Management.

To change the format, in the Directory Connector attribute mapping screen: map the attribute "givenName sn" (or "sn givenName") to "displayName" in the Cisco Cloud Attribute Names column.

Alternatively, map the attribute "sn givenName" to "displayName"

Troubleshoot Directory Connector

Check Directory Connector for Errors

You may receive an email informing you that the Directory Connector is not working.

1 First, ensure that the machine where the connector was installed has connectivity to the network.

2 Run Directory Connector and sign in to the Dashboard.

3 Verify that there are no errors in the Dashboard.

4 Follow the troubleshooting steps.

Related References

Directory Connector Stopped Working

Directory Connector Stopped Working

Problem   You received alert emails notifying you that your Directory Connector is not working.

Possible Cause

- The Directory Connector may not be installed correctly.

- The Directory Connector may not be running.

- The network may not be available.

Solution   Try the following:

- Open the Control Panel, then Programs and Features. Locate Directory Connector. If it's not there, download the latest version and install it.

- Open Service and locate Cisco DirSync Service. Make sure that it displays the status as Started. If the service is stopped, right-click and select Start to restart the service.

- Make sure the server on which you installed the Directory Connector has the access to Internet.

Error Messages and Fixes for Directory Connector Synchronization

After the Directory Connector synchronizes user information, it may send you an email report that lists any problems with the synchronization.

Warning or Error Message	Example	How to Fix
Synchronization deletes all existing full administrators.	Synchronization deletes all existing full administrators. Promote other users to full administrator status or change your synchronization configuration.	Create a user in your Active Directory with the same email address as the administrator that you registered in Cisco Cloud Collaboration Management
For [user dn (distinguished name)], the attribute [attribute name] has the following invalid value [attribute value].	For CN=b,OU=Employees,OU=C Users,DC=c,DC=com, the attribute [telephone number] has the following invalid value: +. This attribute must contain at least one number.	An attribute for this user does not have a valid value. Fix its value according to the description in the warning message. Then do another synchronization.
The required attribute [attribute_name] when	The required attribute email address is missing. When adding on-premises entry	One of the required attributes is missing for

adding on-premises entry [user dn (distinguished name)]. The entry is not created in Cisco Cloud Collaboration Management until all required attributes have a value.	[CN=Sales User,OU=Engineers,OU=K,DC=k,DC=local], the entry is not created in Cisco Cloud Collaboration Management until all required attributes have a value.	the user [user_email_address]. Provide the required values for that user.
No on-premises user matches the existing full administrators in Cisco Cloud Collaboration Management. The following cloud full administrators would have been deleted, but were not: [admin email address].	No on-premises user matches the existing full administrators in the cloud. The following cloud full administrators would have been deleted, but were not: [admin email address].	Create a user in your Active Directory with the same email address as the administrator that you registered though Cisco Cloud Collaboration Management
There is a naming conflict for [user dn] for an existing cloud entry object with the name: [user email address], and of user type [user_type].	There is a naming conflict for [CN=M R,OU=Users,OU=D,DC=d,DC=local] with an existing cloud entry object with the name [user_email_address] and of [user_type]. (Unwilling to allow the client to enter value [user email address] for [attribute uid] which conflicts with another user.)	A user with that email address already exists in Cisco Cloud Collaboration Management.

New and Changed Information

Date	Changes Made
June 15, 2017	Added a section for troubleshooting service account sign in issues.
June 5, 2017	Added Windows 2016 to the list of supported servers. Added an example to the connector policy section.
May 4, 2017	Retired the "Best Practices" section and created "Manage Cisco Spark User Accounts" and "Troubleshoot Directory Connector."
March 6, 2017	Added steps to uninstall and deregister directory connectors. Added information about high availability (HA) for failover intervals.
November 23, 2016	Added minimum requirements for RAM and storage.
November 4, 2016	Updated Installing Directory Connector, Launch the Event Viewer, and Enable Troubleshooting.
August 15, 2016	Updated section on using web proxy.
August 8, 2016	Updated Key Combinations. Added a section on using web proxy. Added a note on uninstalling high availability instances. Removed steps in Uninstall the Cisco Directory Connector.
June 3, 2016	Added a section on AD LDS. Added details on disable synchronization.
May 16, 2016	Added a section on Logging into the Cisco Directory Connector.
Feb. 9, 2016	Added section on auto-upgrade.
Nov. 30, 2015	Added Appendix A Mapping Active Directory User Attributes. Corrected Threshold trigger information. Added cross-reference to Appendix in user attribute section.
Nov. 12, 2015	Added required firewall HTTS port setting (port 443).
Oct 15, 2015	Added Directory Connector and AD compatibility information.
Oct 9, 2015	Added "Configure an Avatar" and "Troubleshooting" sections.

Visibility: ⊘ Cisco Cloud Collaboration Management • **7424 Views**

Last modified on Jun 23, 2017 6:04 AM

Tags: directory connector   synchronize users   dirsync   directory synchronization

identity management

Categories: Hybrid Services   Manage Users

0 Comments

Related Content

📄 Cisco Directory Connector Guide for Administrators (PDF)

📄 Deploy Cisco Spark Hybrid Call Service Aware

📄 Deploy Hybrid Calendar Service for On-Premises Microsoft Exchange

📄 Deploy Hybrid Calendar Service for Office 365

📄 Deploy Cisco Spark Hybrid Call Service Aware and Connect

Recommended Content

📄 No Image on a Screen Connected to a Room Device

📄 Adjust Camera Settings on Your Room System from a Touch Controller

📄 Adjust Camera Settings on Your Room Device with a Remote Control

📄 Turn Room Device Speaker Tracking On or Off

📄 Connect to a Cisco Spark Room Device Manually

Incoming Links

📄 Deploy Cisco Spark Hybrid Call Service Aware and Connect

📄 Deploy Cisco Spark Hybrid Call Service Aware

Getting Started with Cisco Spark Hybrid Services