Synchronizing Processors Users and Domains

Synchronizing Processors, Users, and Domains Overview

There are three types of synchronizations in Cisco Prime Collaboration Provisioning:

- Infrastructure Synchronization—Discovers all the objects in the device that Cisco Prime Collaboration Provisioning uses and that are not specific to individual users. The infrastructure data are the configurations that are required to exist on the device before Cisco Prime Collaboration Provisioning can configure user services.

- User Synchronization—Discovers all objects related to individual users.

- Domain Synchronization—Puts existing users discovered during user synchronization into the Domain.

Synchronizing the data in Cisco Unified Communications Manager and Cisco Unity systems, and then synchronizing with the Domains, populates Cisco Prime Collaboration Provisioning with the existing active users and services, and provides a consolidated view of all of the infrastructure and user information.

Remember the following before running any synchronization:

- Infrastructure and user synchronizations retrieve information from the device. They are unidirectional synchronizations. Provisioning does not update devices during these synchronizations. Infrastructure and user synchronizations should be completed on all devices before a Domain synchronization is started.

- You can execute the synchronizations independently and in any order. However, to preserve the integrity of the data, it is recommended that you run the synchronizations consecutively, and in the following order:

  1. Infrastructure synchronization.

  2. User synchronization.

- After a new Provisioning installation, the infrastructure synchronization must be executed first. You should not run more than one synchronization at a time.

- Ensure that you have checked the connectivity of the device. Click **Test Connection** (under Actions) from the Device details Quick View before running any synchronization. The test results appear in the Device details Quick View.

- The test connection results must be successful before synchronizing Unified Message Processors. If you start synchronization for a Unified Message Processor when the test connection status is "In Progress" or "Failure", the synchronization will fail.

- After a Call Processor or Unified Message Processor is synchronized, do not change the type of device. For example, if you add a Cisco Unified Communications Manager, do not change the Call Processor type to Cisco Unified Communications Manager Express.

- After a Domain synchronization, you can use Cisco Prime Collaboration Provisioning to directly manage the individual user account. You no longer have to use the underlying Cisco Unified Communications Manager or Cisco Unity systems.

- Any out-of-band configurations (meaning configurations that are performed directly on the processor but not synchronized with Provisioning) can result in failed orders. You must always keep Cisco Prime Collaboration Provisioning synchronized with the processors that it is provisioning.

Note When you click on Device's infrastructure or user synchronization, a popup window appears with the message 'Start Synchronization will put the system into maintenance mode'.

If you click **OK**, the system enters into maintenance mode and then the sync starts. Once the sync completes, the system comes out of the maintenance mode automatically.

If you click **Cancel**, the system does not enter into maintenance mode and the sync does not start.

If a parallel sync is already running, then the system waits for the other sync activity to complete and then comes out of the maintenance mode.

Change Notification feature will be automatically enabled for Cisco Unified Communications Manager 10.0 and above versions. This feature is not supported for Cisco Unified Communications Manager versions less than 10.0.

Note From 10.6 release, Change Notification feature is supported when the Cisco Prime Collaboration Provisioning is running in maintenance mode.

Any updates to infrastructure or user configuration of Cisco Unified Communications Manager will be automatically synchronized to Provisioning every 5 minutes. This avoids the need for daily or frequent synchronization with Cisco Unified Communications Manager.

As part of change notification, the user records are also updated to include the newly added services. To view the start and end time of change notification synchronization for a Cisco Unified Communications Manager, launch the quickview and click View Detailed Log in the Actions pane.

The following services and infrastructure objects are automatically synchronized from Cisco Unified Communications Manager, through the Change Notification feature:

- Call Park
- Call Pickup Group
- CallManagerGroup
- CSS
- CmcInfo
- CommonPhoneConfig
- CommonDeviceConfig
- Conference Now
- CTIRoutePoint
- Device Profile
- DateTimeGroup
- DeviceMobility
- Endpoint
- Emergency Location (ELIN) Group
- FacInfo
- GeoLocation
- Hunt List
- Hunt Pilot
- H323Gateway
- Line
- Line Group
- Location
- MediaResourceList
- MediaResourceGroup
- MeetMe
- PhysicalLocation
- Remote Destincation Profile
- Route List
- Route Pattern
- RoutePartition
- Route Group
- SIPProfile
- SIPTrunk
- TransPattern
- UcService
- User
- VoiceMail Profile
- VoiceMail Pilot
- VG224
- VG310
- VG320

Infrastructure and User Synchronization

You use the infrastructure synchronization to synchronize the infrastructure data in the devices. The infrastructure synchronization retrieves device information that is used across multiple users.

To synchronize infrastructure configuration products and users:

Procedure

Step 1	Choose **Device Setup**.
Step 2	Hover over Quick View of the device for which you want to run synchronization.
Step 3	Do one of the following:

- To initiate Infrastructure Synchronization, click **Start Infrastructure Synchronization**
- To initiate User Synchronization, click **Start User Synchronization**

The progress of synchronization is displayed in the Quick View under Synchronization Status.

Step 4	Click **View Detailed Logs**.

A synchronization log is created, listing the objects that could not be assigned. It also shows a warning message if an unknown element is received from the device. This log is replaced each time a synchronization occurs.

Note   If you see the warning message "Skipped unexpected element," you can ignore it. The message indicates that Provisioning does not support the item that was sent back from the device.

If the status of an infrastructure or user synchronization does not change for an extended period of time, verify that the Nice service is running.

If the Nice service is stopped, restart the service, and then restart the infrastructure or user synchronization.

If you wish to manage the Analog Phones, you have to update the ipt.properties file. In this file, update the dfc.ipt.cisco.callmanager.analog_phone_support to Y and then do the user synchronization. You must restart Provisioning after the user synchronization is completed.

For the list of Cisco Unified Communications Manager objects that Provisioning synchronizes, see Cisco Unified Communications Manager Objects that Are Synchronized, on page 5.

You use the infrastructure synchronization to synchronize the unified messaging infrastructure data in Provisioning with the Unified Message Processor:

- SubscriberTemplate—A Subscriber Template in Cisco Unity Connection, and the e-mail message processor.
- UnifiedMessagingFeatureSpecification—A class of service in Cisco Unity Connection, and the e-mail message processor.

You use the user synchronization to synchronize the unified messaging user data in Provisioning with the Unified Message Processor.

- UMInfo—A user in Cisco Unity Connection, and Cisco Unity Express in conjunction with their user's voicemail and e-mail information.

- VoiceMailInfo—A user in Cisco Unity Connection, and Cisco Unity Express in conjunction with UMInfo and EmailInfo.

- EmailInfo—A user in Cisco Unity Connection in conjunction with VoiceMailInfo and UMInfo.

Note If during the synchronization of Cisco Unity Express you encounter device connection errors, close all Telnet sessions on the Cisco Unity Express system and restart the synchronization. Cisco Unity Express only allows one Telnet session at a time. Cisco Prime Collaboration Provisioning cannot synchronize with a Cisco Unity Express device that has another telnet session open.

Note If you observe that the synchronization is not progressing, click the **Stop Stuck Synchronization** link to terminate the selected infra or user synchronization.. The system creates a log about this event in the Audit Logs. Stop Stuck synchronization option does not work if the process runs successfully.

Note PCP monitors the Device (infra/user) sync status every one hour. If the sync remains stuck for one hour, the configured user gets an email notification. Audit trail is updated with the following message and the synchronization stops:

'Automatic synchronization status check Failed'.

Note IM and Presence 9.0 and higher versions are integrated with Cisco Unified Communications Manager. Due to this, user synchronization will be disabled for IM and Presence 9.0 and higher versions. User information will be directly synchronized from Cisco Unified Communications Manager.

For IM and Presence, use the Infrastructure synchronization to synchronize the User Settings Infrastructure data with Provisioning.

Note After upgrading your Cisco Unified Communications Manager, you must perform User Synchronization manually to synchronize change notification settings.

Cisco Unified Communications Manager Objects that Are Synchronized

The following tables list the Cisco Unified Communications Manager objects that are synchronized during an infrastructure and user synchronization in Provisioning.

Table 1: Cisco Unified Communications Manager Objects Synchronized During an Infrastructure Synchronization

• AAR Group	• Gatekeeper	• Partition	• SIP Trunk
• Call Park	• Geo Location	• Phone Profile	• SIP Profile
• Calling Search Space	• Geo LocationConfiguration	• Phone Template	• Softkey Template
• Client Matter Codes	• Geo Location Filter	• Presence Group	• SRST
• Cisco Unified CM Group	• Hunt Group	• Physical Location	• Translation Pattern
• Call Pickup Group	• Hunt List	• Region	• UC Service Profile
• Common Device Config	• Hunt Pilot	• Remote Destination Profile	• VG202
• Conference Bridge	• H323 Gateway	• Resource Priority Namespace List	• VG204
• Conference Now	• H323 Trunk	• Resource Priority Namespace Network Domain	• VG224
• Date Time Setting	• Interactive Voice Response (IVR)	• Route Filter	• VG310
• Date/Time Group	• Line Group	• Route Group	• VG320
• Device Mobility Info	• Location	• Route List	• VG350
• Device Mobility Group	• MLPP Domain	• Route Partition	• VGVoicemail Pilot
• Device Pool	• Media Resource Group	• Route Pattern	• Voicemail Port
• Device Profile	• Media Resource List		• Voicemail Profile
• Dial Plan	• Meet-Me Number/Pattern		
• Dial Plan Tag	• Message Waiting		
• Digit Discard Instruction	• MOH Audio Source		
• Enable Password Router			
• Emergency Location (ELIN) Group			
• Forced Authorization Codes			

Table 2: Cisco Unified Communications Manager Objects Synchronized During User Synchronization

• Calling Search Space	• IP Phone	• Line	• Remote Destination Profile
• Device Pool	• License Capabilities	• Location	• Remote Destination Profile Line
• Directory Number		• Phone	• User

Error Messages While Synchronizing a Call Processor

Some of the error messages you encounter while synchronizing a call processor:

The Detailed Log page lists items that could not be synchronized from the Cisco Unified Communications Manager device. For example, on the page, you will see the following message:

```
Completed. But the following objects could not be
synchronized: [SecurityProfile, DialPlanTag, SIPTrunk, PhoneTemplate, DigitDiscardInstruction]
```

Incomplete synchronization can occur because of the following:

- Network problems that did not allow the items to be properly synchronized. To determine if this is the cause, analyze the nice.log file. A network problem can be the cause if the file displays the following information:

```
java.security.PrivilegedActionException:com.sun.xml.messaging.saaj.SOAPExceptionImpl:Message
 send failed.
```

- Configuration issues with the items. In this case, copy the nice.log file and contact the Engineering Team.

Overview of Domain Synchronization

Domain synchronization aggregates data from synchronizations. Devices are not accessed during a Domain synchronization.

During a Domain synchronization, Cisco Prime Collaboration Provisioning does the following:

- Synchronizes users and their services with the Provisioning inventory, creates new users, and updates the records.

- Synchronizes user accounts and updates Cisco Prime Collaboration Provisioning so that users can log in (logins are created only if the self-care rule is enabled; see Business Rule Descriptions.

- Associates services to Service Areas.

- Synchronizes the assigned voicemail directory numbers in Unity Connection or Unity Express to those in Cisco Unified Communications Manager.

Business rules determine the criteria used for synchronizing Domains (see Configuring Business Rules for Domain Synchronization, on page 11).

To fully synchronize a Domain, you must perform an infrastructure and user synchronization for each device in the Domain, and then perform a Domain Synchronization.

Note If a device in the Domain is already synchronized, it is recommended that a Domain synchronization also be done.

While running Domain synchronization, remember the following:

- If you use a user synchronization on Cisco Unified Communications Manager Express to add users to Provisioning, the first name, last name, phone number, and department data are not obtained by Provisioning. The Manage Users page, displays "Unknown" in these fields.

  You can update the user information through Provisioning, but be aware that this information will be pushed to the Cisco Unified Communications Manager Express system, and will overwrite any existing information for the user in the ephone description field.

- You should not run more than one synchronization at a time. Run all synchronizations sequentially.

- If a Cisco Unified Communications Manager Express is the only device present in a Domain and Service Area, during Domain synchronization users are not created in Provisioning if the ephone username command is not configured in Cisco Unified Communications Manager Express. Ensure that the ephone username command is configured in Cisco Unified Communications Manager Express for all users.

- A device profile is added to a user's record as an Extension Mobility Access product only if the device profile is subscribed to the extension mobility service in Cisco Unified Communications Manager.

- If the Cisco Unified Communications Manager and Cisco Unified Presence added to the service area are upgraded to 9.0 versions, the following services will be removed from the user records:

  - Enable Presence

  - Enable Presence Client

  - Client User Settings

    The user records will be updated with the User Services product details.

- Cisco Prime Collaboration Provisioning allows you to provision device profiles with services enabled or disabled at enterprise level.

  If a device profile has associated services, the device profile will be associated to a user only if a matching service URL is found.

  Note   Extension Mobility service can be associated to a user, even if the device profile has no associated services or if the services are enabled at enterprise level.

- Cisco Prime Collaboration Provisioning allows you to provision device profiles with services enabled or disabled at enterprise level.

  If a device profile has associated services, the device profile will be associated to a user only if a matching service URL is found.

- After domain synchronization, all services related to users are updated in the user record. You can change, cancel or edit services related to users without configuring a service area.

- In an upgraded server, you must run the user synchronization followed by domain synchronization to remove the Email services and merge Unified Messaging service with Voicemail.

Synchronizing Domains

To synchronize domains:

Procedure

Step 1   Choose **Provisioning Setup**.

Step 2   From the Domains table, hover over quick view of the Domain you want to synchronize, and click **Start Domain Synchronization**.

A popup appears saying that the Domain Synchronization has started successfully. The Last Synchronization field in Quick View displays the status of synchronization along with the start and completion time.

Domain synchronization cannot be started without configuring synchronization rules.

Note   If you observe that the synchronization is not progressing, click the **Stop Stuck Synchronization** link to terminate the selected domain or LDAP synchronization. The system creates a log about this event in the Audit Logs. Stop Stuck synchronization option does not work if the process runs successfully.

Note   PCP monitors the Domain sync status every one hour. If the sync remains stuck for one hour, the configured user gets an email notification. Audit trail is updated with the following message and the synchronization stops:

'Automatic synchronization status check Failed'.

Note   For Cisco Prime Collaboration Provisioning 12.3 and later, after the domain synchronization is completed, if admin and globaladmin users exist in any of the devices, then those users are restricted during user sync operation.

Related Topics

Configuring Business Rules for Domain Synchronization, on page 11

Overview of Domain Synchronization, on page 7

Business Rules for Domain Synchronization, on page 10

Change Notification

Change notification allows you to sync information and includes maximum number of scenarios where the information is synced from Unified Communications Manager to Cisco Prime Collaboration Provisioning.

However, in certain cases, when you perform provisioning from Unified Communications Manager directly, information isn't synced in Cisco Prime Collaboration Provisioning after the change notification.

To remove data inconsistencies between the Cisco Prime Collaboration Provisioning and the Unified Communications Manager, we highly recommend that you use Cisco Prime Collaboration Provisioning to perform all provisioning activities. We don't recommend that you use Unified Communications Manager to perform provisioning.

For Cisco Prime Collaboration Provisioning 12.3 and later

Note When you add users to Unified Communications Manager, change notification updates all users except admin and globaladmin in Cisco Prime Collaboration Provisioning.

Business Rules for Domain Synchronization

Business rules determine the criteria used for adding users to a Domain.

For Domain synchronization to work properly, you must configure at least one of the following rules:

- Sync All Users (Unified CM)—If enabled, all user accounts in all of the Call Processors in the Domain are assigned to the Domain being synchronized. This rule overrides the Match Department rule.

- Sync Only Existing Users—If enabled, the Domain synchronization does not create new users. Only services of existing users in the Domain are synchronized.

- Sync by Attribute—You have the following options:

  - Match Department—If enabled, the Domain synchronization associates only the Call Processor user accounts whose department code matches one in the list specified in the rule configuration.

  - Match Location—If enabled, the Domain synchronization associates only the Call Processor user accounts whose phone location matches one in the list specified in the rule configuration.

  - Match Device Pool—If enabled, the Domain synchronization associates only the Call Processor user account whose Phone or Remote Destination Profile has a device pool value that matches one in the list specified in the rule configuration.

The rest of the Domain synchronization rules coreside (do not have a priority level) with the above rules. Following are the coresident Domain synchronization rules:

- Sync All Users (Unity Connection)—If this rule is enabled, all user accounts in a given Message Processor are assigned to a Provisioning Domain. Otherwise, only user accounts in the given Message Processor with a matching Call Processor user account are assigned.

- Sync Primary User From Unity Connection—If enabled, user information is updated from the associated Message Processor account; otherwise it is updated from the Call Processor.

  Note If you try to run a Domain synchronization when none of the required rules are enabled, a message appears in the Synchronize Domain page stating that you are required to enable one of the rules. You can click the Configure Synchronization Rules link on this page to open the Configure Domain Sync Rules page, where you can configure the desired Domain synchronization rule. For more information, see Overview of Domain Synchronization.

If more than one of the required rules are enabled, only one of the rules will be in effect.

The rule priority is applied in the following order:

1. Sync All Users (Unified CM)

2. Sync Only Existing Users

3. Match Department

4. Match Location

5. Match Device Pool

If Sync All Users (Unified CM) rule is enabled, the settings of all the other rules are ignored. If Sync Only Existing Users rule is enabled, the settings for the last three rules are ignored. The last three rules are additive, meaning that if two of the rules are enabled, then only users that satisfy both constraints are synchronized.

Configuring Business Rules for Domain Synchronization

For Domain synchronization to work properly, you must configure Domain synchronization business rules.

Tip A description of each business rule appears when you place your cursor over the information icon next to the rule.

Procedure

Step 1 Choose **Provisioning Setup**.

Step 2 In the Domains listing page, select a Domain and click **Edit**.

Step 3 Scroll down to the Synchronization Rules area on the Domain Configuration page.

Step 4 Select the required rules.

You must select at least one Call Processor synchronization rule for the domain synchronization to work properly. If you select the Sync by Attribute rule, you must select at least one of the options listed under Sync by Attribute rule.

For more information on Domain synchronization rules, see Business Rules for Domain Synchronization, on page 10.

Step 5 Click **Save**.

Domain Synchronization Log Messages

This section provides explanations for some of the messages that can appear in the Domain Synchronization Log report.

Duplicate username encountered. So skipping the creation of this user: TestUser from the Call Processor: TestCCM

Indicates that another user exists in Provisioning with the same ID, but the ID uses a different case. Services which belong to this user will not be synchronized.

To fix this problem, remove one of the users from Cisco Unified Communications Manager.

No matching voicemail info found for directory number 123400000

The synchronization could not find a voicemail for the directory number. This problem can occur when either a synchronization was not run on the Unified Message Processor (so the voicemails are not present in Provisioning), or no matching voicemail information was found for the directory number.

To fix this problem, either run user synchronization on the Unified Message Processor, or create a Service Area with the correct settings.

The device profile line Line 1 - 123400000 could not be added to the customer record because a service area with the following properties could not be determined in the domain Cisco: Call Processor: TestCCM

A device profile line could not be assigned to a Service Area with the listed settings.

To fix this problem, either create a Service Area with the same settings or change the line settings on Cisco Unified Communications Manager.

For Blocking Users

If admin and globaladmin users are restricted during user sync operation, then, the information about the restricted users appears in the log.

Schedule Synchronization

For Cisco Prime Collaboration Release 11.1 and later

Using Schedule Synchronization, you can synchronize Call Processors, Message Processors, Presence Processors, Active Directories, and Domains.

The **Schedule Synchronization** page lists the existing jobs along with its job name, start synchronization time, frequency, job status, synchronization status, and logs. You can click **View** under the logs column to view synchronization log file of the job. Using these log files, you can analyze the cause of synchronization failure. You also have options to add, delete, edit, and run the job immediately.

Prerequisite: You must have administrator privilege to perform this task.

Note After upgrading to Cisco Prime Collaboration Provisioning 11.1, all cron jobs (scheduled for synchronization) from the system are migrated as synchronization jobs to the **Schedule Synchronization** page. These jobs will be displayed with the job status as scheduled.

To add schedule synchronization job:

Procedure

Step 1 Choose **Administration** > **Schedule Synchronization**.

Step 2 Click **Add** to create a new synchronization job for the device.

Step 3 In the **Create New Synchronization Schedule** window, enter the required details. Refer Table 3: Schedule Synchronization Configuration Fields for field descriptions.

Step 4 Click **Synchronization Preview** to run the script without performing any synchronization and to display the list of processors and domains that will be synchronized in the **Preview Synchronization Log**. Using synchronization preview logs, you can easily identify and correct syntax errors in custom granular synchronization data.

Step 5 Click **Save and Run Now** to execute the job immediately. If you do not want to execute the job immediately, you can choose **Save and Close** option.

- To edit an existing job, check the required job name and click **Edit**. Make the necessary changes and click **Save and Run Now**.

- To delete one or more jobs, check the required job name and click **Delete**.

- To execute one or more synchronization jobs immediately, check the required job name and click **Run Now**.

- To cancel an existing job, check the required job name and click **Cancel**.

Note
- You can cancel multiple synchronization jobs simultaneously if synchronization status is in progress.

- Job status will be displayed as "canceled" after the cancel is completed.

- Job status will be displayed as "canceling" while cancel is in progress.

- Synchronization status will not be available for a canceled job.

Note When any infrastructure or user scheduled sync starts, the system enters into maintenance mode automatically and exits when the sync completes.

If a parallel sync is already running, then the system waits for the other sync activity to complete and then comes out of the maintenance mode.

Table 3: Schedule Synchronization Configuration Fields

Field	Description
Job Name	Unique job name. Accepted charters are alphanumeric(A-Z, a-z, 0-9), space, underscore(_), and hyphen(-).

Synchronize Every	Frequency at which the synchronization job should run.
	Choose one of the following type and enter a numeric value in the text box for options except One Time:
	• One Time
	• Hour(s)
	• Day(s)
	• Week(s)
	By default, **One Time** is selected.
Start Date	Choose the date and time when the synchronization operation must start.
	By default current client date and time is displayed.
Synchronization Type	Click the appropriate configuration method.
	• Synchronization Schedule Builder—Click **Synchronization Schedule Builder**, when you want to perform mass synchronization of the processors. Both infrastructure and subscriber synchronization are run for each processor.
	• Custom Granular Synchronization—Click **Custom Granular Synchronization**, when you want to synchronize specific processor.
Synchronization Schedule Builder	You can invoke mass synchronization operation for,
	• All
	• All Call Processors
	• All Message Processors
	• All IMPs
	• All LDAPs
	• All Domains
	By default, option **All** is checked.

Custom Granular Synchronization	Granular Synchronization invokes synchronization operations for objects specified in the text area.
	The data should be in the format:
	<object class>.<object name>: <sync type>
	The valid values are:
	• *object class* : cp (Call Processor), mp (Message Processor), pp (Presence Processor), ad (Active Directory), or domain.
	• *object name* : all or specific object name.
	• *sync type* : infra(infrastructure), sub(subscriber), or both.
	For example :
	• cp.Test-UCM: infra
	• mp.all: sub
	• pp.all: both - equivalent to the [presenceprocessor] mass sync
	• ad.all: - ActiveDirectory mass sync
	• domain.Test-Dom:
Synchronization Options	You can check the required synchronization option from the following:
	• Force Domain Synchronization—Allows the domain synchronization to be performed even after the device synchronization failure.
	• Run Device Synchronization in Parallel—Runs synchronization for all the devices in parallel.
	• Abort Synchronization on Device Synchronization Failure—Instructs the script to quit after a synchronization failure

Configuring Directory Search Synchronization Source

To configure user data service (UDS), you must set the directory source. Directory source can be either LDAP server or Call Processor. If LDAP server is set as the directory source, UDS will be disabled in Cisco Prime Collaboration Provisioning. By default, LDAP server is set as the directory source. For enabling UDS, you must set the directory source as Call Processor.

You cannot enable UDS, if any of the Call Processor is integrated with LDAP. After enabling UDS, if a LDAP integrated Call Processor is added to Cisco Prime Collaboration Provisioning, Cisco Prime Collaboration Provisioning will disable the UDS automatically by setting the directory source as LDAP server.

The processor against which the first service is ordered for a user will be set as the home cluster for the user.

If UDS is enabled, when a user is removed from the home cluster, Provisioning will delete the corresponding user details from the other Call Processor clusters.

You can enable directory search synchronization while adding a new Call Processor or choose to do it later.

To configure the directory search synchronization source:

Procedure

Step 1   Choose **Advanced Provisioning** > **Unified Communication Services**.

Step 2   Click **Use Communication Manager for Directory Data**.

Step 3   Click **Apply**.

A warning message is displayed stating directory search synchronization will add the user details to all Call Processors that are 10.x and above. Depending on the number of users, this operation may take several hours and may impact system performance.

Step 4   Click **Yes** to continue.

Enable button appears next to **Use Communication Manager for Directory Data** option.

Step 5   Click **Enable** for directory search synchronization to happen.

Note   After clicking **Enable** and on adding the call processors if the sync is not auto-initiated then you must manually initiate the sync from UCS or disable and re-enable Directory Search. This may take several hours to complete.

Unified Communication Services page will be updated to show the synchronization status for each affected cluster. If synchronization fails, an error message and links to the log files will be displayed.

Synchronizing an LDAP Server with Provisioning

You can synchronize the accounts in a Lightweight Directory Access Protocol (LDAP) server with Cisco Prime Collaboration Provisioning. Cisco Prime Collaboration Provisioning can use this information to create new users accounts in itself automatically, update already existing user information, or delete users.

Cisco Prime Collaboration Provisioning can populate its user database with user IDs directly from an associated LDAP source. Configuring and scheduling LDAP synchronization are done through domain configuration.

You can configure a filter query at the domain level to allow Cisco Prime Collaboration Provisioning to identify the exact users that have to be imported into Cisco Prime Collaboration Provisioning, as opposed to importing the entire LDAP directory into each domain. You can create complex filters based on the available fields in Microsoft Active Directory.

Administrators can control how Cisco Prime Collaboration Provisioning removes users. They can configure the "Always Delete" option when a user is no longer in the LDAP directory so that when the synchronization between Cisco Prime Collaboration Provisioning and Active Directory runs, the user will be removed from Cisco Prime Collaboration Provisioning and the user's services will be moved to the global namespace. The "Delete if user has no services" option prevents a user from being deleted if the user still has associated

services. These optional settings can help remove unused services and free directory numbers after employees have left a company.

![Note icon]

Note If users are not given admin privileges in AD, they cannot write to the DN.

The following table shows the step-by-step workflow to add and synchronize an LDAP server with Cisco Prime Collaboration Provisioning.

Table 4: LDAP Workflow in Provisioning

Step	Task and Description
Step 1	Configuring Provisioning to Use LDAP and ACS Servers In this step, you can configure Cisco Prime Collaboration Provisioning to connect to an LDAP or ACS server to authenticate, read, and synchronize.
Step 2	Adding LDAP Server, on page 18 In this step, you add details such as device name, IP Address, admin distinguished name and user search base. You also choose the suitable server type.

Step	Task and Description
Step 3	Configuring LDAP Server Synchronization, on page 21
	Note Before you configure LDAP settings and perform synchronization, refer the following sections under Before LDAP Synchronization, on page 19 for more understanding.
	• Greenfield Deployments
	• Brownfield Deployments
	• General Information About LDAP Synchronization
	In this step, you select a Domain and the Directory Source you have configured in the Device Setup page. Then, you configure the information Cisco Prime Collaboration Provisioning gets from these servers in the settings pane. These settings synchronize and authenticate the users from the Directory/ACS server to Cisco Prime Collaboration Provisioning.
	You also schedule synchronization and then choose the domain, and start LDAP Synchronization.
	LDAP Synchronization Report, on page 35
	You can find explanations for some of the messages that can appear in the LDAP Synchronization report.

Adding LDAP Server

To add LDAP server in Cisco Prime Collaboration Provisioning:

Procedure

Step 1 Choose **Device Setup**.

Step 2 Click **Add** to add devices to Cisco Prime Collaboration Provisioning.

Step 3 In the Add Device window, enter the necessary information such as Name and IP address.

Note For the device name, valid values are space, alphanumeric characters (A-Z, a-z, 0-9), underscore (_), hyphen (-), period (.), and at sign (@).

Refer Adding Devices for field descriptions of Call Processor Fields, Unified Message Processor Fields and LDAP and ACS Server Configuration Fields.

Step 4 In the Application drop-down list , select Directory Server (LDAP) and choose the suitable LDAP Server Type. For more information on the server type, see LDAP and ACS Server Configuration Fields table.

Step 5   If the Active Directory is enabled for secure connection, check **Use SSL** checkbox and change the Server Port to 636. For non-secure connection, the Server Port field is populated with 389 by default.

> **Note**   LDAP port when LDAP server is a Global Catalog server:
>
> - 3268—When SSL is not required.
>
> - 3269—When SSL is required. (If you enter this port number, make sure that you check the **Use SSL** check box.)

Step 6   Enter details of Backup Server IP Address and Backup Server Port as appropriate.

Step 7   Enter details of LDAP manager in Admin Distinguished Name and Admin Password fields. The Admin Distinguished Name field contains details of the user who has admin privileges in Active Directory.

> **Note**
> - For Admin Distinguished Name, be sure to use complete canonical name, for example, CN= Administrator, OU =Sales, DC=ca, DC=com.
>
> - Refer Distinguished Names for more information on how to configure the Distinguished Names.
>
> - For more information on Admin Distinguished Name, see LDAP and ACS Server Configuration Fields table.
>
> - Admin user account entered in "Admin Distinguished Name" should have permissions to perform read and write operations.

Step 8   Enter CN or OU search base details in LDAP User Search Base of an administrator. For more information on LDAP User Search Base, see LDAP and ACS Server Configuration Fields table.

Step 9   Click **Save**.
Test Connection validates details entered as part of Device Setup and gives a Success or Failure message.

Before LDAP Synchronization

Before you configure LDAP settings and perform synchronization, refer the following sections for more understanding.

Greenfield Deployments

For greenfield deployments, remember the following:

When a service is ordered for a user that is imported from LDAP server, the Getting Started Wizard pushes the LDAP server details like LDAP directory, authentication and system settings to Cisco Unified Communications Manager. Cisco Unified Communications Manager marks the user as LDAP user. The users that are marked as LDAP user can log into the Self-Care portal of Cisco Unified Communications Manager, using the credentials configured in the LDAP server.

> **Note**   After you upgrade to latest version of Cisco Prime Collaboration Provisioning, you must run LDAP synchronization in Provisioning. Otherwise, LDAP imported users will not be marked as LDAP users in Cisco Unified Communications Manager.

Brownfield Deployments

For brownfield deployments, you must do the following:

1. Create an Infrastructure template (Advanced Provisioning > Batch Provisioning > Add > Add Batch Actions > AddLDAPAuthentication.txt or ChangeLDAPAuthentication.txt batch files) for LDAP authentication to disable authentication in Cisco Unified Communications Manager (you must choose the option "No" for "Use LDAP Authentication for End Users" attribute). Push this configuration to Cisco Unified Communications Manager through batch project.

Note **From Cisco Prime Collaboration Provisioning 11.6 and later**

- You can access all templates under the **Batch Provisioning** menu option.

- System does not provide Configuration template feature.

2. Create an Infrastructure template for LDAP System to disable LDAP synchronization in Cisco Unified Communications Manager. You must provide the value, "sAMAccountName" for "LDAP Attribute for User ID" field, if you have selected Microsoft AD server. You must provide the value, "uid" for "LDAP Attribute for User ID" field, if you have selected Microsoft ADAM or Lightweight Directory Services. Push this configuration to Cisco Unified Communications Manager through batch project.

3. Create an Infrastructure template for LDAP authentication to enable authentication in Cisco Unified Communications Manager again (you must choose the option "Yes" for "Use LDAP Authentication for End Users" attribute). Push this configuration to Cisco Unified Communications Manager through batch project.

4. You must run Infrastructure synchronization from Provisioning UI to identify LDAP directory in Cisco Unified Communications Manager, before you start provisioning the services for users in Cisco Prime Collaboration Provisioning.

Note Single LDAP synchronization is compatible with Cisco Unified CM 10.5.1 and above only.

General Information About LDAP Synchronization

- Cisco Prime Collaboration Provisioning allows writing DN back to the LDAP server.

- The following servers are supported as LDAP servers:

  - Microsoft Active Directory servers 2000, 2003, and 2008

  - Open LDAP

  - Oracle Directory

  - AD 2012

- LDAP synchronization only creates the users; it does not add their services to their user records. Make sure you run domain synchronization after LDAP synchronization so that the users' services are added to their user records.

> • The user search base configured in LDAP services in the domain is used to synchronize LDAP users into the Cisco Prime Collaboration Provisioning user database.
>
> • You cannot delete an LDAP server which is associated to a Domain. You must remove the LDAP server from the Domain to delete it.

Configuring LDAP Server Synchronization

To Configure LDAP Server Synchronization:

Procedure

Step 1   Choose **Provisioning Setup**.

Step 2   In the Domains pane, select a Domain and click **Edit**.

Step 3   On the Domain Configuration page, select the Directory Source that is configured on the Device Setup page.

Step 4   In the settings pane, you configure the information Cisco Prime Collaboration Provisioning gets from the servers by entering or choosing the details as suitable in the respective fields. These settings are used to synchronize and authenticate the users from the Directory/ACS server to Prime Collaboration.

The LDAP Settings pane contains the following sub-panes:

> • LDAP Sync Policy
>
> • LDAP Field Mappings
>
> • Domain LDAP Filters
>
> • Service Area LDAP Filters
>
> • User Role LDAP Filters
>
> • Write Back LDAP Settings

For more information on LDAP Sync Policy and Field Mappings sub-panes, see the Table 5: LDAP Settings Fields table.

While synchronizing users from the LDAP server, you can use the Domain, Service Area, and User Role LDAP filters when the User Type is enabled for Automatic Service Provisioning. These filters help identify the default Service Area and User Role to be used during Automatic Service Provisioning.

For more information on LDAP Filters, see the Table 7: LDAP Synchronization Filters table.

Step 5   For all the changes on the LDAP server to be synchronized to Cisco Prime Collaboration Provisioning, select the following:

> • Mode—**Authentication and Synchronization** under LDAP Sync Policy sub-pane.
>
> • Update existing user details—**All fields** under LDAP Sync Policy sub-pane.
>
> • Action when LDAP users deleted—**Delete user only** under LDAP Sync Policy sub-pane.
>
> • User Search base—Enter a user search base under LDAP Sync Policy sub-pane.
>
> > • Unlike Cisco Unified CM, Cisco Prime Collaboration Provisioning supports only one user search base for a domain. However, you can create multiple domains for multiple user searches.

- When adding an LDAP user in Cisco Unified CM through Provisioning UI, the user search base in Provisioning domain and Unified Communications Manager must be the same.

- Filter query for synchronization—Synchronize all users. Cick the **Edit** icon under Domain LDAP Filters sub-pane and choose the necessary detail. Click **Save**.

Step 6 Click **Save**.

Note PCP monitors the LDAP sync status every one hour. If the sync remains stuck for one hour, the configured user gets an email notification. Audit trail is updated with the following message and the synchronization stops:

'Automatic synchronization status check Failed'.

Scheduling and Performing LDAP Synchronization

To schedule synchronization, set the **Synchronization Interval** and **Synchronization Start Date** in the LDAP Settings pane.

After saving the Domain Configuration page, select the Domain and hover over Quick view. Select **Start LDAP Synchronization**.

You can view the LDAP synchronization details in the domain quick view. You can click the **View Detailed Log** option available in the domain **Quick View** to view LDAP synchronization logs.

After an LDAP synchronization, a report is created. The report lists the operations that could not be performed during synchronization. Operation failure can be due to incorrect data entered into the LDAP server or incorrect user settings.

You cannot delete an LDAP server which is associated to a Domain. Remove the LDAP server from the Domain to delete it.

The following table provides details about the LDAP Configuration fields.

Table 5: LDAP Settings Fields

Field	Description
Mode	- Authentication Only—The LDAP server is used only for user authentication. - Authentication and Synchronization—The LDAP server is used both to provide user authentication and to obtain user information.
Update Existing User Details	- All fields—If any user information is changed in the LDAP server, the same information is updated in Provisioning. - Do not update—User information in Provisioning is not updated when there are changes to the user information in the LDAP server.

Field	Description
Action for stale LDAP users	**Note** A stale LDAP user is a user account that no longer matches the user search base and/or the Domain LDAP filters. • Do not make changes in Provisioning—The corresponding user in Cisco Prime Collaboration Provisioning is not deleted. • Delete user if there are no services in Provisioning—The corresponding user in Cisco Prime Collaboration Provisioning is also deleted, if the user does not have any services in Cisco Prime Collaboration Provisioning. The user is not deleted in Cisco Prime Collaboration Provisioning, if the user has any services in Cisco Prime Collaboration Provisioning. • Delete user in Provisioning—The corresponding user in Cisco Prime Collaboration Provisioning is also deleted, even if the user has any services in Cisco Prime Collaboration Provisioning. • Delete user, but keep services in Provisioning and CUCM—The corresponding user is deleted in Cisco Prime Collaboration Provisioning and Cisco Unified Communications Manager. • Delete user and all services from Provisioning and CUCM—The corresponding users and their services are deleted in the device and in Cisco Prime Collaboration Provisioning. The user is deleted in Cisco Prime Collaboration Provisioning and Cisco Unified Communications Manager, if the user is not an LDAP user in Cisco Unified Communications Manager. The user is deleted in Cisco Unified Communications Manager, if the user is an LDAP user in Cisco Unified Communications Manager.

Field	Description
User Search Base	The user search base of a domain. Provisioning searches for users under the base under Active Directory. For example, CN=Users, DC=Cisco, DC=com. This search base is used only for LDAP synchronization. In the Microsoft Active Directory server, you can use the command dsquery user to list the complete user search base. **Note** Cisco Prime Collaboration Provisioning supports only one user search base per domain.
(For Cisco Prime Collaboration Provisioning 11.5 and later) Sync Inactive (Disabled) Users	Synchronizing disabled users enables you, as an administrator, to manage disabled LDAP user accounts, and autoprovision services. When this check box is checked, LDAP Sync pulls the disabled LDAP users. Applicable when the **LDAP Sync Policy** Mode is **Authentication and Synchronization**. Applicable only for Microsoft Active Directory server or Microsoft ADAM or Lightweight Directory Services. Not configurable through the Getting Started Wizard. Mapping of user roles for disabled users is same as for active LDAP users. If disabled users are not synchronized even though Sync Inactive (Disabled) Users is enabled, you may have set the advanced query not to synchronize the disabled users. It is recommended not to use "msDS-UserAccountDisabled" attribute in the advanced query.

Field	Description

Field Mapping	Lists which user fields in Cisco Unified Communications Manager correspond to certain LDAP user fields. The only fields that you can configure in Cisco Prime Collaboration Provisioning are the following:
	
	   • Contact phone number—Select either telephone number or ipPhone.
	
	   • Contact email—Select either mail or sAMAccountName.
	
	   • User ID—User ID can be mapped to the following fields in LDAP server:
	
	      • employeeNumber
	
	      • mail
	
	      • sAMAccountName
	
	      • telephoneNumber
	
	      • userPrincipalName
	
	   • Middle Name—Select either middleName or initials.
	
	   • Directory URI—Select mail, msRTCSIP-primaryuseraddress, or none.
	
	For a list of all field mapping between Provisioning and the LDAP server, see Table 6: LDAP Field Mapping, on page 28.

Field	Description
Filter Query for Synchronization	

Field	Description
	• Synchronize all users—All users are synchronized.
	• Simple query—You can configure a query by using a combination of the following fields:
	• User ID
	• Department
	• Contact phone number
	• Title
	• First Name
	• Last Name
	• Manager ID—Provide a manager ID that is fully qualified as in the Active Directory integration. For example, a user, John Doe with user ID jdoe is: CN=jdoe,*<user search base>*
	• Directory URI
	• Contact email
	• City
	• State
	• Office
	• Company
	• Street
	• P. O. Box
	• Zip Code
	• Country
	• Fax Number
	• IP Phone Number
	• You can use an asterisk (*) for a partial string search.
	Advanced query—You can enter any LDAP query; for example: (&(sAMAccountName=johndoe) (department=Cisco*)(mail=john@cisco.com)). You can enter custom attributes in the Advanced

Field	Description
	Query textbox. You can use the advanced query functionality in Automatic Service Provisioning to choose the Service Area to provision the user services in and also for the User Role so that users coming in can be assigned to a particular user role.

✎

Note Using "IN" filter in Automatic Service Provisioning, you can configure multiple queries. For example:

- To fetch multiple Directory Numbers, separate the search string using semicolon. For example: 4930;5930.

- To fetch multiple combinations of Directory Numbers, separate the search string using an asterisk and semicolon. For example: 40105*;40116*;40127*;.

- For contact phone numbers, you can use:

    - '+' symbol in search criteria such as +44*

    - '/+' symbol in search criteria such as /+44*

- For contact phone numbers, using "IN" filter with multiple values in search criteria with comma as delimiter, you can use '/+' symbol such as /+44*, /+55*,/+33*.

- Similarly, using "IN" filter you can synchronize multiple users from the LDAP server with comma as delimiter. For example: User1, User2, User3.

- Wildcard character (*) is allowed in the filter, it can be used either in beginning or in the end of the field.

Likewise, you can use '=' and '!=' operators to configure queries. For example, if you provide a single userID:

- The '=' operator synchronizes only that user from the LDAP server.

- The '!=' operator does not synchronize that user alone from the LDAP server. All other users are synchronized.

Using * with userID such as User123* fetches all the users whose id starts with User123.

The table below lists the field mapping between Cisco Prime Collaboration Provisioning and the LDAP server. The data in the specified Provisioning field is synchronized with the user data in the corresponding LDAP field.

Table 6: LDAP Field Mapping

Provisioning Field	LDAP Field
Phone Number	telephoneNumber or ipPhone number.
Note For Provisioning users, if this field is empty, the line directory number is assigned automatically to this field during the time of line ordering.	**Note** For LDAP users, if this field is empty, the line directory number is not assigned to this field during the time of line ordering.

Provisioning Field	LDAP Field
Email	mail
User ID	User ID can be mapped to the following fields in LDAP server: • employeeNumber • mail • sAMAccountName • telephoneNumber • userPrincipalName
First Name	givenName.
Last Name	sn.
Middle Name	middleName or initials
Directory URI	mail, msRTCSIP-primaryuseraddress, or none
Manager ID	manager
Department	department
Title	title
Home Number	homephone
Mobile Number	mobile
Pager Number	pager

Note If you have configured LDAP server type as Microsoft ADAM or Lightweight Directory Services or Oracle directory server or OpenLDAP, uid is listed in the User ID drop-down list instead of sAMAccountName.

Note **(For Cisco Prime Collaboration Release 11.2 and later)** The following LDAP attributes are not supported in the domain user interface for openLDAP and Oracle directory server:

• msRTCSIP-primaryuseraddress

• userPrincipalName

• ipPhone number

• middlename

While synchronizing users from the LDAP server, you can use the following filters when the User Type is enabled for Automatic Service Provisioning. These filters help identify the default Service Area and User Role to be used during Automatic Service Provisioning:

Table 7: LDAP Synchronization Filters

LDAP Filter	Description
Domain LDAP filter	Use this filter to specify which users should be assigned to each domain.
Service area LDAP filter	Use this filter to specify which users should be assigned to each service area. Service area LDAP filter is not enabled if there is no service area configured in that domain. **Note** This filter is only applicable for Auto-Provisioning. **(For Cisco Prime Collaboration Release 11.2 and later)** Cisco Prime Collaboration Provisioning can support the common LDAP attributes in the Service Area LDAP filter by extending the filters to accept advanced queries.

LDAP Filter	Description
Role LDAP filter	Use this filter to specify which User Role should be applied for autoprovisioning the default services. If this filter is not configured, users that are synchronized from the LDAP server are mapped to the default role configured in Business Rules and autoprovisioning happens only if the default User Role in domain Business Rules is enabled for autoprovisioning.
	Both the default User Role and the User Role that matches with the filter is assigned for the user if:
	• The User Role specified in the filter is different from default Business Rule, and
	• The filter criteria matches.
	Note This filter is only applicable for Auto-Provisioning.
	(For Cisco Prime Collaboration Release 11.2 and later) Cisco Prime Collaboration Provisioning can support the common LDAP attributes in User Role LDAP filter by extending the filters to accept advanced queries.
	Service Area and User Role filters are not enabled, if you have selected the synchronization mode as "Authentication Only." Also, both the filters are applied only when autoprovisioning is enabled.

While creating the service area filter, you can configure the following settings:

• Assign new line from the extension block.

• Apply mask to LDAP synchronized telephone numbers. You can enter the mask value that needs to be applied on the LDAP synchronized number in the Mask field. Note the following points while entering the mask value:

    • The valid values for Mask field are 0-9, plus symbol (+), upper case x (X), and backslash followed by plus symbol (\+).

    • It can start with +, \+, X, or numerals (0-9).

    • It can be a combination of numerals and character X (for example, 12XXX, +XX234, XX231XXX).

    • E.164 characters (+ and \+) can be used only at the beginning of the value. These characters should not be used in between the numbers or X.

Provisioning applies the mask to the LDAP synchronized number after removing the non-numeric characters and provisions the line accordingly.

Note	Mask field is enabled only if you have checked the Apply Mask to LDAP Synchronized Telephone Numbers check box.

Mask option is available only for users who are synchronized from the LDAP server. Also, masked numbers are used only during autoprovisioning Line for LDAP users.

- If you have checked the Assign New Line from the Extension Block check box, even if there is an LDAP synchronized number, Provisioning selects the directory number from the DN block and provision the line accordingly.

- If you have checked the Apply Mask to LDAP Synchronized Telephone Numbers check box:

  - When there is no LDAP synchronized number, Cisco Prime Collaboration Provisioning does not provision Line service for the user.

  - When there is LDAP synchronized number, Cisco Prime Collaboration Provisioning applies the mask on LDAP synchronized number and uses the masked number for auto provisioning the line.

- If both the check boxes are checked, LDAP synchronized number is masked and masked DN is used for autoprovisioning the line. If there is no LDAP synchronized number, Cisco Prime Collaboration Provisioning selects a number from the DN block and provision the line accordingly.

- If both the check boxes are unchecked, LDAP synchronized number is used for provisioning the line.

Note	Ensure that the LDAP synchronized number is different from the numbers that are generated in DN Block during autoprovisioning the line.

Write Primary DN to LDAP

For Cisco Prime Collaboration Release 11.2 and later

You can write the Primary DN chosen from Cisco Prime Collaboration Provisioning back to the LDAP server, thus reducing the manual update of the AD fields and masking of DNs. This feature gets triggered at the ordering and domain level.

Note the following points during write-back:

- You can write Primary DN's to AD if LDAP user, Primary DN, and write back settings are enabled at domain level.

- You can perform the write-back while ordering Line and User Services through the user interface and batch.

- You cannot perform the write-back during Cisco Unified CM user synchronization and change notification. If the Primary DN is changed directly in Cisco Unified CM, then you need to wait for the sync / change notification changes to complete and reflect in Cisco Prime Collaboration Provisioning.

- You can configure the write-back settings through domain user interface, and batch.

- You can update the write-back settings through the add or change functionality of batch.

- You cannot configure the write-back settings at domain level through Getting Started Wizard.

Write Back Settings

To write the Primary DN to LDAP, choose **Provisioning Setup** and select a Domain to edit. Expand LDAP Settings pane to view Write Back Settings subpane.

- The system allows you to write-back Primary DN to more than one LDAP attribute at the same time. LDAP attributes to which you can write-back Primary DN are telephoneNumber, ipPhone, and Mobile.

- When you check the required **LDAP Attribute** check box, it enables the corresponding **Apply Mask** field for editing. You can enter the mask value and click **Save**.

- The valid values for **Apply Mask** are 0-9, plus symbol (+), upper case x (X), backslash followed by plus symbol (\+), dash (-), parenthesis (()), space ( ), comma (,), star (*), and period (.). You can use the E.164 characters (+ and \+) only at the beginning of the value.

From the Domains table, hover over **Quick View** of the domain you want to write back, and click **Start Write Back to LDAP**.

Note If the LDAP attribute is set to **Do not write to LDAP**, write back does not happen and **Start Write Back to LDAP** is disabled.

Once **Start Write Back to LDAP** action starts, other actions such as **Start Domain Synchronization** and **Start LDAP Synchronization** are disabled.

Primary DN is not written to LDAP while ordering due to any one of the following reasons:

- LDAP server is unreachable or incorrect LDAP credentials.

- Admin user account entered in "Admin Distinguished Name" does not have permission to perform a write operation.

- The Domain level LDAP attribute is set to **Do not write to LDAP.**

- User does not have any primary directory number.

Check the LDAP test connection and the order status or select any attribute from the LDAP attribute drop-down list.

To view detailed log information, hover over **Quick View** of the desired domain, and then click **View Detailed Log**.

An error message is displayed in the order details page (go to the user record of the user on the **User Provisioning** page) if any error occurred during the write- back. You cannot view the write-back status for all the orders.

Write Directory URI to LDAP

For Cisco Prime Collaboration Provisioning Release 12.6 SU2 and later

You can write the Directory URI back to the LDAP server to support URI dialing with video devices. This feature is triggered at the domain level.

Note the following points during write-back of Directory URI to LDAP:

- Enable LDAP user, Directory URI, and write-back settings at the domain level to write-back Directory URI to LDAP.

- You can perform the write-back while ordering Line and User Services through the user interface and batch.

- If the Directory URI is changed directly in Unified Communications Manager, wait for the sync or change notification to complete and reflect in Cisco Prime Collaboration Provisioning.

Directory URI Write Back Settings

Use this procedure to write-back Directory URI to LDAP.

Before you begin

- From **LDAP Settings** > **LDAP Sync Policy** > **Mode** of the domain, choose **Authentication and Synchronization** to enable **Write back Directory URI to LDAP** section.

- From **LDAP Settings** > **Write-back Directory URI to LDAP** of the domain, check the **msRTCSIPPrimaryuseraddress** check box to allow the write-back.

Procedure

Step 1 From Cisco Prime Collaboration Provisioning, choose **Provisioning Setup**.

Step 2 Click **Start Write Direct URI to LDAP** from the **Quick View** of the domain you want to write-back.

You can see the status of the write-back at the **Write back to LDAP** field on the **Quick View** of the domain.

Note

1. You cannot mask the Direct URI value before write-back.

2. You cannot perform other actions like **Start Domain Synchronization** and **Start LDAP Synchronization**, once the write-back starts.

3. If you perform a write-back when the Directory URI is empty, the write-back action updates the empty value in LDAP.

4. The write-back to LDAP fails when:

   - You do not have the permission to perform a write operation.

   - You have set the domain level LDAP attribute to **Do not write to LDAP**.

   - Directory URI is not available in the user details.

   - The LDAP server does not have the attribute msRTCSIP-primaryuseraddress.

   - The attribute name in the LDAP server does not match msRTCSIP-primaryuseraddress.

5. To view detailed log information, hover over the **Quick View** of the desired domain, and click **View Detailed Log**.

LDAP Synchronization Report

This section provides explanations for some of the messages that can appear in the LDAP Synchronization report.

The following users were not created because they are already present in another Domain: user1, user2

The listed users are present in the LDAP server, but could not be created in Provisioning in the current Domain, because they are already present in another Domain.

To fix this problem, delete the users from the other Domain and run the LDAP synchronization again.

Deletion of User and associated services failed for the following users: UserId, OrderId, Status

This message appears when Delete user with Services is enabled, and deleting the user and services from the device and from Provisioning fails. In order to delete the services in a device, a single order is created for each user and the order status is shown in the above report with the order ID. You have to manually delete these users and corresponding services. You can click on the link provided for the user ID in the above report to access these user records.

The following user and associated services were deleted successfully: UserId, OrderId, Status

This message appears when Delete user with Services is enabled, and deleting the user and services from the device and from Provisioning succeeds.

The following users were not deleted because the delete option was not set: user1 user2

The users were deleted in the LDAP server, but they were not deleted during the LDAP synchronization, since Do not delete is enabled.

To fix this problem, enable either Delete User Only or Delete User with Services option, and run the LDAP synchronization again.

LDAP Synchronization Report