



## Integrate with Directory Sources

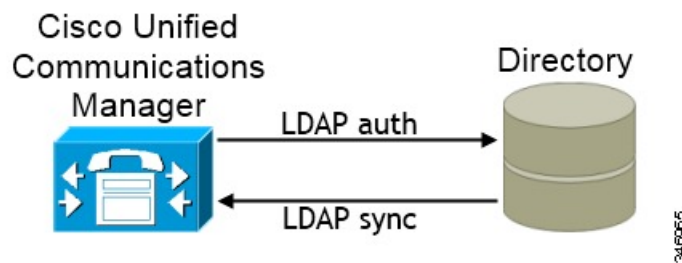
Cisco Jabber integrates with directory sources in on-premises deployments to query for and resolve contact information. Learn why you should enable synchronization and authentication between your directory source and Cisco Unified Communications Manager. Understand how directory integration works with certain contact sources. Review when you should configure the client for directory integration. Find configuration examples of specific integration scenarios.

- [Set Up Directory Synchronization and Authentication](#), page 1
- [Contact Sources](#), page 5
- [Client Configuration for Directory Integration](#), page 13
- [Federation](#), page 36

## Set Up Directory Synchronization and Authentication

When you set up an on-premises deployment, you should configure Cisco Unified Communications Manager to do both of the following:

- Synchronize with the directory server.
- Authenticate with the directory server.



Synchronizing with the directory server replicates contact data from your directory to Cisco Unified Communications Manager.

Enabling authentication with the directory server lets Cisco Unified Communications Manager proxy authentication from the client to the directory server. In this way, users authenticate with the directory server, not with Cisco Unified Communications Manager or a presence server.

### Related Topics

[Configuring Cisco Unified Communications Manager Directory Integration Server Setup Guide](#)

## Synchronize with the Directory Server

Directory server synchronization ensures that contact data in your directory server is replicated to Cisco Unified Communications Manager.

### Enable Synchronization

The first step to synchronize with a directory server is to enable synchronization on Cisco Unified Communications Manager.

#### Procedure

---

- Step 1** Open the **Cisco Unified CM Administration** interface.
  - Step 2** Select **System > LDAP > LDAP System**.  
The **LDAP System Configuration** window opens.
  - Step 3** Locate the **LDAP System Information** section.
  - Step 4** Select **Enable Synchronizing from LDAP Server**.
  - Step 5** Select the type of directory server from which you are synchronizing data from the **LDAP Server Type** drop-down list.
- 

#### What to Do Next

Specify an LDAP attribute for the user ID.

### Populate User ID and Directory URI

When you synchronize your LDAP directory server with Cisco Unified Communications Manager, you can populate the end user configuration tables in both the Cisco Unified Communications Manager and the Cisco Unified Communications Manager IM and Presence Service databases with attributes that contain values for the following:

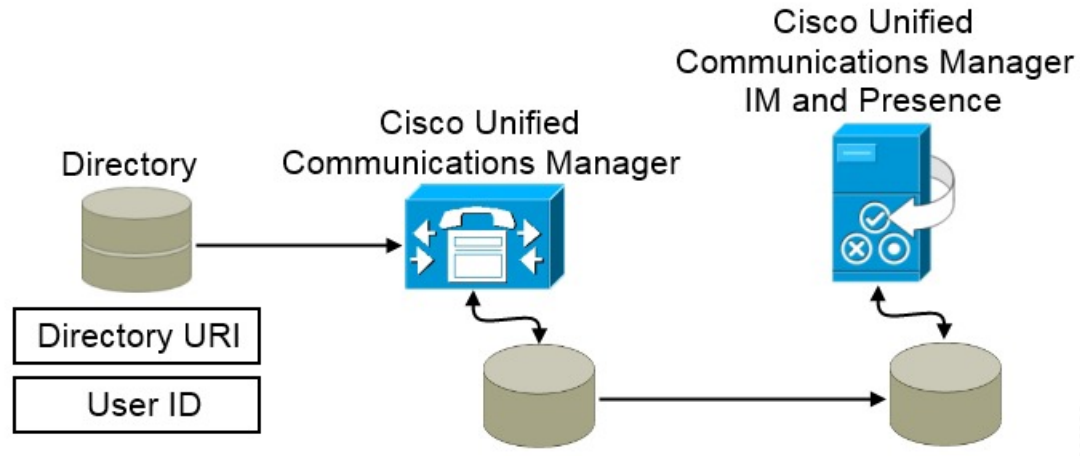
#### User ID

You must specify a value for the user ID on Cisco Unified Communications Manager. This value is required for the default IM address scheme and for users to log in. The default value is sAMAccountName.

## Directory URI

You should specify a value for the directory URI if you plan to:

- Enable URI dialing in Cisco Jabber.
- Use the directory URI address scheme on Cisco Unified Communications Manager IM and Presence Service version 10 and higher.



When Cisco Unified Communications Manager synchronizes with the directory source, it retrieves the values for the directory URI and user ID and populates them in the end user configuration table in the Cisco Unified Communications Manager database.

The Cisco Unified Communications Manager database then synchronizes with the Cisco Unified Communications Manager IM and Presence Service database. As a result, the values for the directory URI and user ID are populated in the end user configuration table in the Cisco Unified Communications Manager IM and Presence Service database.

## Specify an LDAP Attribute for the User ID

When you synchronize from your directory source to Cisco Unified Communications Manager, you can populate the user ID from an attribute in the directory. The default attribute that holds the user ID is `sAMAccountName`.

### Procedure

- Step 1** Locate the **LDAP Attribute for User ID** drop-down list on the **LDAP System Configuration** window.
- Step 2** Specify an attribute for the user ID as appropriate and then select **Save**.

**Important** If the attribute for the user ID is other than `sAMAccountName`, you must specify the attribute as the value for the parameter in your client configuration file as follows:

The BDI parameter is `BDIUserName`.

```
<BDIUserName>attribute-name</BDIUserName>
```

If you do not specify the attribute in your configuration, and the attribute is other than `sAMAccountName`, the client cannot resolve contacts in your directory. As a result, users do not get presence and cannot send or receive instant messages.

---

## Specify an LDAP Attribute for the Directory URI

On Cisco Unified Communications Manager version 9.0(1) and higher, you can populate the directory URI from an attribute in the directory. The default attribute is `msRTCSIP-primaryuseraddress`.

### Procedure

---

- Step 1** Select **System > LDAP > LDAP Directory**.
- Remember** To add or edit an LDAP directory, you must first enable synchronization.
- Step 2** Select the appropriate LDAP directory or select **Add New** to add an LDAP directory.
- Step 3** Locate the **Standard User Fields To Be Synchronized** section.
- Step 4** Select the appropriate LDAP attribute for the **Directory URI** drop-down list.
- Step 5** Select **Save**.
- 

## Perform Synchronization

After you add a directory server and specify the required parameters, you can synchronize Cisco Unified Communications Manager with the directory server.

### Before You Begin

If your environment includes a presence server, you should ensure the following feature service is activated and started before you synchronize with the directory server:

- Cisco Unified Presence: **Cisco UP Sync Agent**
- Cisco Unified Communications Manager IM and Presence Service: **Cisco Sync Agent**

This service keeps data synchronized between the presence server and Cisco Unified Communications Manager. When you perform the synchronization with your directory server, Cisco Unified Communications Manager then synchronizes the data with the presence server. However, the **Cisco Sync Agent** service must be activated and started.

### Procedure

---

- Step 1** Select **System > LDAP > LDAP Directory**.
  - Step 2** Select **Add New**.  
The **LDAP Directory** window opens.
  - Step 3** Specify the required details on the **LDAP Directory** window.  
See the *Cisco Unified Communications Manager Administration Guide* for more information about the values and formats you can specify.
  - Step 4** Select **Save**.
  - Step 5** Select **Perform Full Sync Now**.  
**Note** The amount of time it takes for the synchronization process to complete depends on the number of users that exist in your directory. If you synchronize a large directory with thousands of users, you should expect the process to take some time.
- 

User data from your directory server is synchronized to the Cisco Unified Communications Manager database. Cisco Unified Communications Manager then synchronizes the user data to the presence server database.

## Authenticate with the Directory Server

You should configure Cisco Unified Communications Manager to authenticate with the directory server. When users log in to the client, the presence server routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then proxies that authentication to the directory server.

### Procedure

---

- Step 1** Open the **Cisco Unified CM Administration** interface.
  - Step 2** Select **System > LDAP > LDAP Authentication**.
  - Step 3** Select **Use LDAP Authentication for End Users**.
  - Step 4** Specify LDAP credentials and a user search base as appropriate.  
See the *Cisco Unified Communications Manager Administration Guide* for information about the fields on the **LDAP Authentication** window.
  - Step 5** Select **Save**.
- 

## Contact Sources

In on-premises deployments, the client requires a contact source to resolve directory look ups for user information. You can use the following as a contact source:

### Basic Directory Integration

Basic Directory Integration (BDI) is an LDAP-based contact source.

### Cisco Unified Communications Manager User Data Service

Cisco Unified Communications Manager User Data Service (UDS) is a contact source on Cisco Unified Communications Manager.

UDS is used for contact resolution in the following cases:

- If you configure the `DirectoryServerType` parameter in the client configuration file to use “UDS”. With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.
- If you deploy Expressway for Mobile and Remote Access. With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.



**Note** Cisco Jabber supports UDS using the following Cisco Unified Communications Manager versions:

- Cisco Unified Communications Manager Version 9.1(2) or later with the following COP file: `cmterm-cucm-uds-912-5.cop.sgn`.
- Cisco Unified Communications Manager Version 10.0(1). No COP file is required.

You can deploy approximately 50 percent of the maximum number of Cisco Jabber clients that your Cisco Unified Communications Manager node supports.

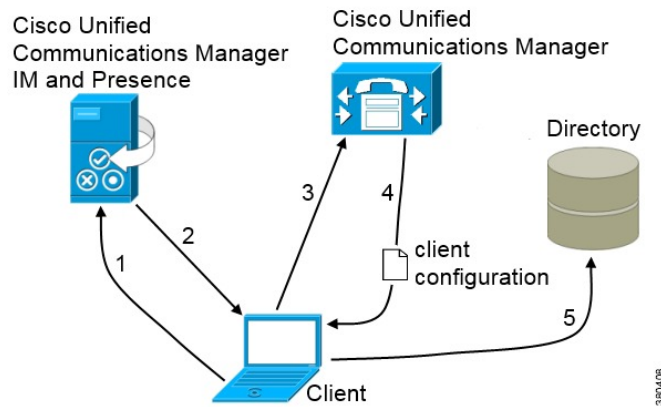
For example, if a Cisco Unified Communications Manager node can support 10,000 Cisco Jabber clients using an LDAP-based contact source, that same node can support 5,000 Cisco Jabber clients using UDS as a contact source.

## Basic Directory Integration

When using Basic Directory Integration (BDI), the client retrieves contact data from the directory service as follows.

- 1 The client connects to the Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service server.
- 2 The client gets the LDAP profile configuration section in the service profile from the Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service server.  
The service profile contains the location of Cisco Unified Communications Manager (TFTP) server. Depending on your configuration, the service profile can also contain the credentials to authenticate with the directory.
- 3 The client connects to the Cisco Unified Communications Manager server.
- 4 The client downloads the client configuration file from the Cisco Unified Communications Manager server.  
The client configuration file contains the location of the directory. Depending on your configuration, the client configuration file can also contain the credentials to authenticate with the directory.

- The client uses the directory location and the authentication credentials to connect to the directory.



## Authentication with Contact Sources

BDI requires users to authenticate with the directory source to resolve contacts. You can use the following methods to authenticate with the contact source, in order of priority:

### Specify credentials in Cisco Unified Presence or Cisco Unified Communications Manager

Specify credentials in a profile on the server. The client can then retrieve the credentials from the server to authenticate with the directory.

This method is the most secure option for storing and transmitting credentials.

### Set common credentials in the client configuration file

You specify a shared username and password in the client configuration file. The client can then authenticate with the directory server.



#### Important

The client transmits and stores these credentials as plain text.

You should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.

### Use anonymous binds

Configure the client to connect to the directory source with anonymous binds.

## Specify LDAP Directory Configuration on Cisco Unified Presence

If your environment includes Cisco Unified Presence version 8.x, you can specify directory configuration in the LDAP profile. The client can then get the directory configuration from the server to authenticate with the directory source.

Complete the steps to create an LDAP profile that contains authentication credentials, and then assign that profile to users.

## Procedure

---

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Unified Personal Communicator > LDAP Profile**.
- Step 3** Select **Add New**.
- Step 4** Specify a name and optional description for the profile in the following fields:
- **Name**
  - **Description**
- Step 5** Specify a distinguished name for a user ID that is authorized to run queries on the LDAP server. Cisco Unified Presence uses this name for authenticated bind with the LDAP server.
- Step 6** Specify a password that the client can use to authenticate with the LDAP server in the following fields:
- **Password**
  - **Confirm Password**
- Step 7** Select **Add Users to Profile** and add the appropriate users to the profile.
- Step 8** Select **Save**.
- 

## What to Do Next

Specify any additional BDI information in the client configuration file.

## Specify LDAP Directory Configuration on Cisco Unified Communications Manager

If your environment includes Cisco Unified Communications Manager version 9.x and higher, you can specify credentials when you add a directory service. The client can then get the configuration from the server to authenticate with the directory source.

Complete the steps to add a directory service, apply the directory service to the service profile, and specify the LDAP authentication configuration for the directory service.

## Procedure

---

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Add a directory service as follows:
- a) Select **User Management > User Settings > UC Service**.  
The **Find and List UC Services** window opens.
  - b) Select **Add New**.  
The **UC Service Configuration** window opens.
  - c) In the **Add a UC Service** section, select **Directory** from the **UC Service Type** drop-down list.
  - d) Select **Next**.
  - e) Specify details for the directory service as follows:



**Product Type**

Select **Directory**.

**Name**

Enter a descriptive name for the server, for example, PrimaryDirectoryServer.

**Description**

Enter an optional description.

**Hostname/IP Address**

Enter the address of the directory server in one of the following formats:

- Hostname
- IP Address
- FQDN

**Protocol Type**

Select one of the following protocols from the following drop-down list:

- TCP
- UDP

f) Select **Save**.

**Step 3** Apply the directory service to your service profile as follows:

a) Select **User Management > User Settings > Service Profile**.

The **Find and List Service Profiles** window opens.

b) Find and select your service profile.

The **Service Profile Configuration** window opens.

c) In the **Directory Profile** section, select up to three services from the following drop-down lists:

- **Primary**
- **Secondary**
- **Tertiary**

d) Specify the credentials that the client can use to authenticate with the LDAP server in the following fields:

- **Username**
- **Password**

e) Select **Save**.

---

## Set Credentials in the Client Configuration

You can set credentials in the client configuration with the following parameters:

- BDIConnectionUsername
- BDIConnectionPassword



### Important

The client transmits and stores these credentials as plain text.

You should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.

The following is an example configuration:

```
<Directory>
  <BDIConnectionUsername>admin@example.com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
</Directory>
```

## Use Anonymous Binds

To use anonymous binds, you set the following parameters in the client configuration file:

Parameter	Value
DirectoryServerType	BDI
BDIPrimaryServerName	IP address FQDN
BDIEnableTLS	True
BDISearchBase1	Searchable organizational unit (OU) in the directory tree
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson
BDIPredictiveSearchFilter	uid or other search filter A search filter is optional.

The following is an example configuration:

```
<Directory>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>True</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIBaseFilter>(&!(objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

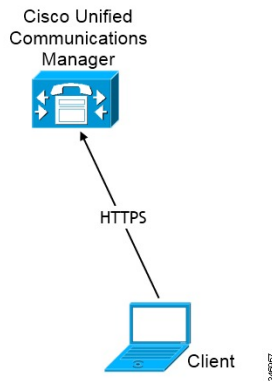
## Cisco Unified Communications Manager User Data Service

UDS is a REST interface on Cisco Unified Communications Manager that provides contact resolution.

UDS is used for contact resolution in the following cases:

- If you set the `DirectoryServerType` parameter to use a value of UDS in the client configuration file. With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.
- If you deploy Expressway for Mobile and Remote Access. With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.

You synchronize contact data into Cisco Unified Communications Manager from a directory server. Cisco Jabber then automatically retrieves that contact data from UDS.



### Enable Integration with UDS

To enable integration with UDS, perform the following steps:

#### Procedure

- 
- Step 1** Create your directory source in Cisco Unified Communications Manager.
- Step 2** Synchronize the contact data to Cisco Unified Communications Manager. After the synchronization occurs, your contact data resides in Cisco Unified Communications Manager.
- Step 3** For manual connections, specify the IP address of the Cisco Unified Communications Manager User Data Service server to ensure that the client can discover the server. The following is an example configuration for the Cisco Unified Communications Manager User Data Service server:
- ```
<UdsServer>11.22.33.44</UdsServer>
```
- Step 4** Configure the client to retrieve contact photos with UDS. The following is an example configuration for contact photo retrieval:
- ```
<UdsPhotoUriWithToken>http://server_name.domain/%uid%.jpg</UdsPhotoUriWithToken>
```

## Set UDS Service Parameters

You can set service parameters for UDS on Cisco Unified Communications Manager.

### Procedure

- 
- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **System > Enterprise Parameters**.  
The **Enterprise Parameters Configuration** window opens.
- Step 3** Locate the **User Data Service Parameters** section.
- 

### UDS Service Parameters

Set values for the following service parameters to configure UDS:

Parameter	Description
<b>Enable All User Search</b>	Allows searches for all users in the directory (search with no last name, first name, or directory number specified). The default value is true.
<b>User Search Limit</b>	Limits the number of users returned in a query. The default value is 64.
<b>Number of Digits to Match</b>	Specifies the number of digits to match when users search for phone numbers. <b>Tip</b> To resolve PSTN numbers, you should set the value as equal to the number of digits in the PSTN numbers. For example, if the PSTN numbers have 10 digits, set the value to 10.

## Contact Resolution with Multiple Clusters

For contact resolution with multiple Cisco Unified Communications Manager clusters, you should synchronize all users on the corporate directory to each cluster. You should then provision a subset of those users on the appropriate cluster.

For example, your organization has 40,000 users. 20,000 users reside in North America. 20,000 users reside in Europe. Your organization has the following Cisco Unified Communications Manager clusters for each location:

- `cucm-cluster-na` for North America

- `cucm-cluster-eu` for Europe

In this example, you should synchronize all 40,000 users to both clusters. You then provision the 20,000 users in North America on `cucm-cluster-na` and the 20,000 users in Europe on `cucm-cluster-eu`.

When users in Europe call users in North America, Cisco Jabber retrieves the contact details for the user in Europe from `cucm-cluster-na`.

When users in North America call users in Europe, Cisco Jabber retrieves the contact details for the user in North America from `cucm-cluster-eu`.

## Client Configuration for Directory Integration

Directory integration can be configured through Service Profiles using Cisco Unified Communications Manager 9 or higher or with the configuration file. Use this section to learn how to configure the client for directory integration.




---

**Note**

In instances where a Service Profile and the configuration file are present, settings in the Service Profile take priority.

---




---

**Note**

Cisco Unified Presence 8 profiles cannot be used for directory integration.

---

## Configure Directory Integration in a Service Profile

With Cisco Unified Communications Manager version 9 and higher, you can provision users with service profiles and deploy the `_cisco-uds` SRV record on your internal domain name server.

The client can then automatically discover Cisco Unified Communications Manager and retrieve the service profile to get directory integration configuration.

To set up service discovery to support service profiles, you must:

- Deploy the `_cisco-uds` SRV record on your internal domain name server.
- Ensure that the client can resolve the domain name server address.
- Ensure that the client can resolve the hostname of Cisco Unified Communications Manager.
- Ensure that the client can resolve the fully qualified domain name (FQDN) for the Cisco Unified Communications Manager.

Cisco Jabber now supports Cisco Unified Communications Manager User Data Service (UDS). In addition to being able to deploy Cisco Jabber using LDAP to connect to Active Directory, Jabber can now alternatively be deployed with Cisco Unified Communications Manager User Data Services contact lookup service. Server scaling must be considered when using the UDS server. A Cisco Unified Communication node can support UDS contact service connections for 50% of the maximum device registrations supported by the server.

To configure directory integration in a service profile, do the following:

## Procedure

- 
- Step 1** Open the **Unified CM Administration** interface.
- Step 2** Add a directory service.
- Select **User Management > User Settings > UC Service**.  
The **Find and List UC Services** window opens.
  - Select **Add New**.  
The **UC Service Configuration** window opens.
  - Select **Directory** from the **UC Service Type** menu and then select **Next**.
  - Set all appropriate values for the directory service and then select **Save**.
- Step 3** Apply the directory service to a service profile.
- Select **User Management > User Settings > Service Profile**.  
The **Find and List Service Profiles** window opens.
  - Select **Add New**.  
The **Service Profile Configuration** window opens.
  - Add the directory services to the directory profile.
  - Select **Save**.
- 

## Directory Profile Parameters

The following table lists the configuration parameters you can set in the directory profile:

Directory Service Configuration	Description
<b>Primary server</b>	Specifies the address of the primary directory server.  This parameter is required for manual connections where the client cannot automatically discover the directory server.
<b>Secondary server</b>	Specifies the address of the backup directory server.
<b>Use UDS for Contact Resolution</b>	Specifies if the client uses UDS as a contact source.  <b>Note</b> By default, UDS provides contact resolution when users connect to the corporate network through Expressway for Mobile and Remote Access.
<b>Use Logged On User Credential</b>	Specifies if the client uses the logged on username and password.  <b>True</b> Use credentials. This is the default value.  <b>False</b> Do not use credentials. Specify credentials with the <code>BDIConnectionUsername</code> and <code>BDIConnectionPassword</code> parameters.

Directory Service Configuration	Description
<b>Username</b>	<p>Lets you manually specify a shared username that the client can use to authenticate with the directory server.</p> <p>If you must use this parameter, you should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.</p>
<b>Password</b>	<p>Lets you manually specify a shared password that the client can use to authenticate with the directory server.</p> <p>If you must use this parameter, you should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.</p>
<b>Search Base 1</b>	<p>Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which the client executes a search.</p> <p>By default, the client searches from the root of the directory tree. You can specify the value of up to three search bases in your OU to override the default behavior.</p> <p>Active Directory does not typically require a search base. You should specify search bases for Active Directory only for specific performance requirements.</p> <p>You must specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory.</p> <p><b>Tip</b> Specify an OU to restrict searches to certain user groups. For example, a subset of your users have instant messaging capabilities only. Include those users in an OU and then specify that as a search base.</p>
<b>Base Filter</b>	<p>Specifies a base filter for Active Directory queries.</p> <p>Specify a directory subkey name only to retrieve objects other than user objects when you query the directory.</p> <p>The default value is (&amp; (objectCategory=person) .</p>
<b>Predictive Search Filter</b>	<p>Defines filters to apply to predictive search queries.</p> <p>You can define multiple, comma-separated values to filter search queries.</p> <p>The default value is ANR.</p>

### Attribute Mappings

It is not possible to change the default attribute mappings in a service profile. If you plan to change any default attribute mappings, you must define the required mappings in a client configuration file.

## Summary of Directory Integration Configuration Parameters

This topic lists all the parameters you can specify to configure directory integration.

The following table lists the parameters you can use for attribute mapping with LDAP directory servers:

<b>Attribute Mapping Parameters</b>	
<ul style="list-style-type: none"> <li>• BDICommonName</li> <li>• BDIDisplayName</li> <li>• BDIFirstname</li> <li>• BDILastname</li> <li>• BDIEmailAddress</li> <li>• BDISipUri</li> <li>• BDIPhotoSource</li> <li>• BDIBusinessPhone</li> <li>• BDI MobilePhone</li> <li>• BDIHomePhone</li> <li>• BDIOtherPhone</li> <li>• BDIDirectoryUri</li> </ul>	<ul style="list-style-type: none"> <li>• BDI Title</li> <li>• BDI CompanyName</li> <li>• BDI UserAccountName</li> <li>• BDI DomainName</li> <li>• BDI Country</li> <li>• BDI Location</li> <li>• BDI Nickname</li> <li>• BDI PostalCode</li> <li>• BDI City</li> <li>• BDI State</li> <li>• BDI StreetAddress</li> </ul>

The following table lists the parameters you can use to connect to an LDAP directory server:

<b>Directory Server Connection Parameters</b>	
<ul style="list-style-type: none"> <li>• BDILDAPServerType</li> <li>• BDI PresenceDomain</li> <li>• BDI PrimaryServerName</li> <li>• BDI ServerPort1</li> </ul>	<ul style="list-style-type: none"> <li>• BDI UseJabberCredentials</li> <li>• BDI ConnectionUsername</li> <li>• BDI ConnectionPassword</li> <li>• BDI EnableTLS</li> </ul>

The following table lists the parameters you can use for contact resolution and directory queries with LDAP directory servers:



**Contact Resolution and Directory Query Parameters**

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>• BDIBaseFilter</li> <li>• BDIUseANR</li> <li>• BDIPredictiveSearchFilter</li> <li>• BDIsearchBase1</li> </ul> | <ul style="list-style-type: none"> <li>• BDIPhotoUriSubstitutionEnabled</li> <li>• BDIPhotoUriSubstitutionToken</li> <li>• BDIPhotoUriWithToken</li> <li>• BDIUseSIPURIToResolveContacts</li> <li>• BDIUriPrefix</li> <li>• BDIDirectoryUri</li> <li>• BDIDirectoryUriPrefix</li> </ul> |
|---|---|

**Summary of UDS Parameters**

The following table lists the parameters you can use to connect to UDS and perform contact resolution and directory queries.

**UDS Parameters**

- |  |
|--|
| <ul style="list-style-type: none"> <li>• DirectoryServerType</li> <li>• PresenceDomain</li> <li>• UdsServer</li> <li>• UdsPhotoUriWithToken</li> </ul> |
|--|

## Directory Integration Parameters

The following sections lists details about the parameters you can configure for LDAP-based directory integration.

### Attribute Mapping Parameters

The following table describes the parameters for mapping LDAP directory attributes:

Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDICommonName	cn	Yes	Yes	No
BDIDisplayName	displayName	Yes	Yes	Yes
BDIFirstname	givenName	Yes	Yes	Yes

Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDILastname	sn	Yes	Yes	Yes
BDIEmailAddress	mail	Yes	Yes	Yes
BDISipUri <b>Note</b> The client uses this parameter for intradomain federation, not URI dialing.	msRTCSIP-PrimaryUserAddress	Yes	Yes	Yes
BDIPhotoSource	thumbnailPhoto	No	No	No
BDIBusinessPhone	telephoneNumber	Yes	No	No
BDIMobilePhone	mobile	Yes	No	No
BDIHomePhone	homePhone	Yes	No	No
BDIOtherPhone	otherTelephone	Yes	No	No
BDIDirectoryUri <b>Note</b> The client uses this parameter for URI dialing.	mail	Yes	No	No
BDITitle	title	Yes	No	No
BDICompanyName	company	Yes	Yes	No
BDIUserAccountName	sAMAccountName	Yes	Yes	Yes
BDIDomainName	dn	Yes	Yes	No
BDICountry	co	Yes	No	No
BDILocation	location	Yes	No	No
BDINickname	displayName	Yes	Yes	Yes
BDIPostalCode	postalCode	Yes	No	No
BDICity	l	Yes	Yes	No
BDIState	st	Yes	Yes	No
BDIStreetAddress	streetAddress	Yes	No	No

## Attributes on the Directory Server

You must index attributes on your LDAP directory server so that the client can resolve contacts.

If you use the default attribute mappings, ensure the following attributes are indexed:

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber

Additionally, ensure you index the following attributes for secondary number queries:

- otherTelephone
- mobile
- homePhone
- msRTCSIP-PrimaryUserAddress

You should index msRTCSIP-PrimaryUserAddress for intradomain federation only.

## Directory Connection Parameters

The following table describes parameters for configuring your LDAP directory connection:

Parameter	Value	Description
BDILDAPServerType	AD OpenLDAP	Specifies the type of LDAP directory server to which the client connects.  <b>AD</b> Connect to Active Directory. This is the default value.  <b>OpenLDAP</b> Connect to OpenLDAP.

Parameter	Value	Description
BDIPresenceDomain	Domain of the presence server	<p>Required parameter. Specifies the domain of the presence server.</p> <p>The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the following user ID: <code>amckenzie</code>. You specify <code>example.com</code> as the presence server domain.</p> <p>When the user logs in, the client constructs the following IM address for Adam McKenzie: <code>amckenzie@example.com</code>.</p>
BDIPrimaryServerName	IP address FQDN	<p>Required parameter. Specifies the address of the primary directory server.</p> <p>This parameter is required for manual connections where the client cannot automatically discover the directory server.</p> <p><b>Note</b> Each time the client starts, it attempts to connect to the primary server. The client attempts to connect to the secondary server if:</p> <ul style="list-style-type: none"> <li>• The primary server is not available.</li> <li>• The primary server fails after the client connects to it.</li> </ul> <p>If the connection to the secondary server is successful, the client keeps the connection to the secondary server until the next restart.</p> <p>If the secondary server fails while the client is connected to it, the client attempts to connect to the primary server.</p>
BDIServerPort1	Port number	Specifies the port for the primary directory server.

Parameter	Value	Description
BDIUseJabberCredentials	true false	<p>Specifies whether the client can use the presence server credentials to sign in to the directory server.</p> <p><b>True</b></p> <p>The client searches for the username and password in this order:</p> <ol style="list-style-type: none"> <li>1 Client configuration file (BDIConnectionUsername and BDIConnectionPassword)</li> <li>2 Presence server</li> </ol> <p>If the credentials are not present, the client tries to sign in anonymously.</p> <p><b>False</b></p> <p>This is the default value. The client tries to sign in using the values of BDIConnectionUsername and BDIConnectionPassword in client configuration file. If those parameters are not present, the client tries to sign in anonymously.</p>
BDIConnectionUsername	Username	<p>Lets you manually specify a shared username that the client can use to authenticate with the directory server.</p> <p><b>Important</b> The client transmits and stores this username as plain text.</p> <p>If you must use this parameter, you should use only a well-known or public set of credentials. The account that you use for integration should have read-only permissions to the directory.</p>
BDIConnectionPassword	Password	<p>Lets you manually specify a shared password that the client can use to authenticate with the directory server.</p> <p><b>Important</b> The client transmits and stores this password as plain text.</p> <p>If you must use this parameter, you should use only a well-known or public set of credentials. The account that you use for integration should have read-only permissions to the directory.</p>

Parameter	Value	Description
BDIEnableTLS	true false	Use TLS to secure directory connections.  <b>true</b> Use TLS.  <b>false</b> Do not use TLS. This is the default value.

## Directory Query Parameters

The following table describes parameters for configuring how the client queries your LDAP directory:

Parameter	Value	Description
BDIBaseFilter	Base filter	Specifies a base filter for Active Directory queries.  Specify a directory subkey name only to retrieve objects other than user objects when you query the directory.  The default value is ( <code>&amp;objectCategory=person</code> ).  Configuration files can contain only valid XML character entity references. Use <code>&amp;amp;</code> instead of <code>&amp;</code> if you specify a custom base filter.
BDIUseANR	true false	Specifies if Cisco Jabber issues a query using Ambiguous Name Resolution (ANR) when it performs a predictive search.  <b>true</b> Use ANR for predictive search. This is the default value.  <b>false</b> Do not use ANR for predictive search. You should set the value to false if you integrate with a directory source other than Active Directory.  <b>Important</b> You must configure your directory server to set attributes for ANR if you want the client to search for those attributes.

Parameter	Value	Description
BDIPredictiveSearchFilter	Search filter	<p>Defines filters to apply to predictive search queries.</p> <p>You can define multiple, comma-separated values to filter search queries.</p>
BDISearchBase1	Searchable organizational unit (OU) in the directory tree	<p>Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which the client executes a search.</p> <p>By default, the client searches from the root of the directory tree. You can specify the value of up to five search bases in your OU to override the default behavior.</p> <p>Active Directory does not typically require a search base. You should specify search bases for Active Directory only for specific performance requirements.</p> <p>You must specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory.</p> <p><b>Tip</b> Specify an OU to restrict searches to certain user groups.</p> <p>For example, a subset of your users have instant messaging capabilities only. Include those users in an OU and then specify that as a search base.</p>

### Related Topics

[Ambiguous Name Resolution for LDAP in Windows 2000](#)

[LDAP Referrals](#)

[Common Default Attributes Set for Active Directory and Global Catalog](#)

### Base Filter Examples

The following are example base filters you can use to look up specific locations or objects.

Find only specific groups:

```
(& (objectClass=user) (memberOf=cn=group-name, ou=Groups, dc=example, dc=com))
```

Find a nested group within a group:

```
(& (objectClass=user) (memberOf:search-oid:=cn=group-name, ou=Groups, dc=example, dc=com))
```

Find only enabled accounts and non-administrator accounts:

```
(& (objectCategory=person) (objectClass=user) (!(userAccountControl:search-oid:=2))
(!(sAMAccountName=*_dbo)) (!(sAMAccountName=*-admin)))
```

## Contact Photo Parameters

The following table describes parameters for configuring how the client retrieves contact photos from an LDAP directory:

Parameter	Value	Description
BDIPhotoUriSubstitutionEnabled	true false	Specifies if photo URI substitution is enabled.  <b>true</b> Photo URI substitution is enabled.  <b>false</b> Specifies if photo URI substitution is disabled. This is the default value.



Parameter	Value	Description
BDIPhotoUriSubstitutionToken	Directory attribute	<p>Specifies a directory attribute to insert in the photo URI; for example, <code>sAMAccountName</code>.</p> <p>Only the following attributes are supported for use with the PhotoURISubstitutionToken parameter:</p> <ul style="list-style-type: none"> <li>• Common Name</li> <li>• Display Name</li> <li>• First Name</li> <li>• Last Name</li> <li>• Nickname</li> <li>• Email Address</li> <li>• Photo Source</li> <li>• Business Phone</li> <li>• Mobile Phone</li> <li>• Home Phone</li> <li>• Preferred Phone</li> <li>• Other Phone</li> <li>• Title</li> <li>• Company Name</li> <li>• User Account Name</li> <li>• Domain Name</li> <li>• Location</li> <li>• Post Code</li> <li>• State</li> <li>• City</li> <li>• Street</li> </ul>

Parameter	Value	Description
BDIPhotoUriWithToken	URI	<p>Specifies a photo URI with a directory attribute as a variable value; for example, <code>http://staffphoto.example.com/sAMAccountName.jpg</code>.</p> <p>The parameter applies to LDAP directory integrations.</p> <p>To configure photo URI substitution, you set the directory attribute as the value of <code>BDIPhotoUriSubstitutionToken</code>.</p> <p><b>Restriction</b> The client must be able to retrieve the photos from the web server without credentials.</p>

### Related Topics

[Contact Photo Formats and Dimensions, on page 27](#)

### Contact Photo Retrieval with BDI

Cisco Jabber retrieves and displays contact photos with the following methods.



#### Note

When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in Cisco Jabber.

### URI substitution

Cisco Jabber dynamically builds a URL to contact photos with a directory attribute and a URL template.

To use this method, set the following values in your configuration file:

- 1 Specify `true` as the value of the `BDIPhotoUriSubstitutionEnabled` parameter.
- 2 Specify a directory attribute to use as a dynamic token as the value of the `BDIPhotoUriSubstitutionToken` parameter; for example, `<BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>`
- 3 Specify the URL and the dynamic token as the value of the `BDIPhotoUriWithToken` parameter; for example, `<BDIPhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>`

With the example values in the preceding steps, the `sAMAccountName` attribute might resolve to `msmith` in your directory. Cisco Jabber then takes this value and replaces the token to build the following URL: `http://staffphoto.example.com/msmith.jpg`.

**Binary objects**

Cisco Jabber retrieves the binary data for the photo from your database.

if using binary objects from Active Directory, `BDIPhotoUriWithToken` should not be set.

To use this method to retrieve contact photos, specify the attribute that contains the binary data as the value of the `BDIPhotoSource` parameter in the configuration; for example,

```
<BDIPhotoSource>jpegPhoto</BDIPhotoSource>
```

**PhotoURL attribute**

Cisco Jabber retrieves a URL from a directory attribute.

To use this method to retrieve contact photos, specify the attribute that contains the photo URL as the value of the `BDIPhotoSource` parameter in the configuration; for example,

```
<BDIPhotoSource>photoUri</BDIPhotoSource>
```

**Contact Photo Formats and Dimensions**

To achieve the best result with Cisco Jabber, your contact photos should have specific formats and dimensions. Review supported formats and optimal dimensions. Learn about adjustments the client makes to contact photos.

**Related Topics**

[Contact Photo Parameters, on page 24](#)

*Contact Photo Formats*

Cisco Jabber supports the following formats for contact photos in your directory:

- JPG
- PNG
- BMP
- GIF

**Important**

Cisco Jabber does not apply any modifications to enhance rendering for contact photos in GIF format. As a result, contact photos in GIF format might render incorrectly or with less than optimal quality. To obtain the best quality, you should use PNG format for your contact photos.

*Contact Photo Dimensions***Tip**

The optimum dimensions for contact photos are 128 pixels by 128 pixels with an aspect ratio of 1:1.

The following table lists the different dimensions for contact photos in Cisco Jabber:

Location	Dimensions
Audio call window	128 pixels by 128 pixels

Location	Dimensions
Invitations and reminders, for example: <ul style="list-style-type: none"> <li>• Incoming call windows</li> <li>• Meeting reminder windows</li> </ul>	64 pixels by 64 pixels
Lists of contacts, for example: <ul style="list-style-type: none"> <li>• Contact lists</li> <li>• Participant rosters</li> <li>• Call history</li> <li>• Voicemail messages</li> </ul>	32 pixels by 32 pixels

### Contact Photo Adjustments

Cisco Jabber adjusts contact photos as follows:

#### Resizing

If contact photos in your directory are smaller or larger than 128 pixels by 128 pixels, the client automatically resizes the photos. For example, contact photos in your directory are 64 pixels by 64 pixels. When Cisco Jabber retrieves the contact photos from your directory, it resizes the photos upwards to 128 pixels by 128 pixels.




---

**Tip** Resizing contact photos can result in less than optimal resolution. For this reason, you should use contact photos that are 128 pixels by 128 pixels so that the client does not automatically resize them.

---

## Cropping

Cisco Jabber automatically crops non-square contact photos to a square aspect ratio, or an aspect ratio of 1:1 where the width is the same as the height.

### Portrait orientation

If contact photos in your directory have portrait orientation, the client crops 30 percent from the top and 70 percent from the bottom.

For example, if contact photos in your directory have a width of 100 pixels and a height of 200 pixels, Cisco Jabber needs to crop 100 pixels from the height to achieve an aspect ratio of 1:1. In this case, the client crops 30 pixels from the top of the photos and 70 pixels from the bottom of the photos.

### Landscape orientation

If contact photos in your directory have landscape orientation, the client crops 50 percent from each side.

For example, if contact photos in your directory have a width of 200 pixels and a height of 100 pixels, Cisco Jabber needs to crop 100 pixels from the width to achieve an aspect ratio of 1:1. In this case, the client crops 50 pixels from the right side of the photos and 50 pixels from the left side of the photos.

## UDS Parameters

The following table provides details about the parameters you can use to connect to UDS and perform contact resolution and directory queries.

Parameter	Value	Description
PresenceDomain	Domain of the presence server	<p>Required parameter. Specifies the domain of the presence server.</p> <p>The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the following user ID: <code>amckenzie</code>. You specify <code>example.com</code> as the presence server domain.</p> <p>When the user logs in, the client constructs the following IM address for Adam McKenzie: <code>amckenzie@example.com</code>.</p>
UdsServer	IP address FQDN	<p>Specifies the address of the Cisco Unified Communications Manager User Data Service (UDS) server.</p> <p>This parameter is required for manual connections where the client cannot automatically discover the UDS server.</p>

Parameter	Value	Description
UdsPhotoUriWithToken	URI	<p>Specifies a photo URI with a directory attribute as a variable value; for example, <code>http://www.photo/url/path/%%uid%.jpg</code>.</p> <p>This parameter applies to UDS directory integrations. You must specify this parameter to download contact photos in either of the following cases:</p> <ul style="list-style-type: none"> <li>• If you configure the <code>DirectoryServerType</code> parameter to use UDS. With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.</li> <li>• If you deploy Expressway for Mobile and Remote Access. With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.</li> </ul> <p><b>Restriction</b> The client must be able to retrieve the photos from the web server without credentials.</p>

## Contact Photo Retrieval with UDS

UDS dynamically builds a URL for contact photos with a directory attribute and a URL template.

To resolve contact photos with UDS, you specify the format of the contact photo URL as the value of the `UdsPhotoUriWithToken` parameter. You also include a `%%uid%%` token to replace the contact username in the URL, for example,

```
<UdsPhotoUriWithToken>http://server_name/%%uid%.jpg</UdsPhotoUriWithToken>
```

UDS substitutes the `%%uid%%` token with the value of the `userName` attribute in UDS. For example, a user named Mary Smith exists in your directory. The value of the `userName` attribute for Mary Smith is `msmith`. To resolve the contact photo for Mary Smith, Cisco Jabber takes the value of the `userName` attribute and replaces the `%%uid%%` token to build the following URL:

```
http://staffphoto.example.com/msmith.jpg
```



### Note

When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in Cisco Jabber.

**Important**

- If you deploy Expressway for Mobile and Remote Access, the client automatically uses UDS for contact resolution when users connect to services from outside the corporate network. When you set up UDS contact resolution for Expressway for Mobile and Remote Access, you must add the web server on which you host the contact photos to the HTTP server allow list in your Cisco Expressway-C server configuration. The HTTP server allow list enables the client to access web services inside the corporate network.
- All contact photos must follow the format of the URL you specify as the value of UdsPhotoUriWithToken.

## Contact Photo Formats and Dimensions

To achieve the best result with Cisco Jabber, your contact photos should have specific formats and dimensions. Review supported formats and optimal dimensions. Learn about adjustments the client makes to contact photos.

### Related Topics

[Contact Photo Parameters, on page 24](#)

### Contact Photo Formats

Cisco Jabber supports the following formats for contact photos in your directory:

- JPG
- PNG
- BMP
- GIF

**Important**

Cisco Jabber does not apply any modifications to enhance rendering for contact photos in GIF format. As a result, contact photos in GIF format might render incorrectly or with less than optimal quality. To obtain the best quality, you should use PNG format for your contact photos.

### Contact Photo Dimensions

**Tip**

The optimum dimensions for contact photos are 128 pixels by 128 pixels with an aspect ratio of 1:1.

The following table lists the different dimensions for contact photos in Cisco Jabber:

Location	Dimensions
Audio call window	128 pixels by 128 pixels

Location	Dimensions
Invitations and reminders, for example: <ul style="list-style-type: none"> <li>• Incoming call windows</li> <li>• Meeting reminder windows</li> </ul>	64 pixels by 64 pixels
Lists of contacts, for example: <ul style="list-style-type: none"> <li>• Contact lists</li> <li>• Participant rosters</li> <li>• Call history</li> <li>• Voicemail messages</li> </ul>	32 pixels by 32 pixels

## Contact Photo Adjustments

Cisco Jabber adjusts contact photos as follows:

### Resizing

If contact photos in your directory are smaller or larger than 128 pixels by 128 pixels, the client automatically resizes the photos. For example, contact photos in your directory are 64 pixels by 64 pixels. When Cisco Jabber retrieves the contact photos from your directory, it resizes the photos upwards to 128 pixels by 128 pixels.




---

**Tip** Resizing contact photos can result in less than optimal resolution. For this reason, you should use contact photos that are 128 pixels by 128 pixels so that the client does not automatically resize them.

---



## Cropping

Cisco Jabber automatically crops non-square contact photos to a square aspect ratio, or an aspect ratio of 1:1 where the width is the same as the height.

### Portrait orientation

If contact photos in your directory have portrait orientation, the client crops 30 percent from the top and 70 percent from the bottom.

For example, if contact photos in your directory have a width of 100 pixels and a height of 200 pixels, Cisco Jabber needs to crop 100 pixels from the height to achieve an aspect ratio of 1:1. In this case, the client crops 30 pixels from the top of the photos and 70 pixels from the bottom of the photos.

### Landscape orientation

If contact photos in your directory have landscape orientation, the client crops 50 percent from each side.

For example, if contact photos in your directory have a width of 200 pixels and a height of 100 pixels, Cisco Jabber needs to crop 100 pixels from the width to achieve an aspect ratio of 1:1. In this case, the client crops 50 pixels from the right side of the photos and 50 pixels from the left side of the photos.

## Directory Server Configuration Examples

This section describes supported integration scenarios and provides example configurations.

### UDS Integration

To integrate with UDS, set the following parameters.

Parameter	Value
DirectoryServerType	UDS
UdsServer	IP address of the UDS server
UdsPhotoUriWithToken	Contact photo URL



#### Note

Configure the DirectoryServerType parameter to UDS only if you want to use UDS for all contact resolution (that is, from inside and outside the corporate firewall).

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>UDS</DirectoryServerType>
  <UdsServer>11.22.33.444</UdsServer>
  <UdsPhotoUriWithToken>http://server-name/%%uid%.jpg</UdsPhotoUriWithToken>
</Directory>
```

## LDAP Integration with Expressway for Mobile and Remote Access

When you deploy Expressway for Mobile and Remote Access with an LDAP directory integration, the client uses:

- LDAP when inside the corporate firewall
- UDS when outside the corporate firewall



### Note

LDAP is the default configuration, so it is not necessary to include the `DirectoryServerType` parameter in your client configuration file.

To ensure that the client can resolve contact photos from both inside and outside your corporate firewall, set the following parameters.

Parameter	Value
<code>BDIPhotoUriWithToken</code>	Contact photo URL when inside the corporate firewall
<code>UdsPhotoUriWithToken</code>	Contact photo URL when outside the corporate firewall

The following is an example configuration:

```
<Directory>
  <BDIPhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg
  </BDIPhotoUriWithToken>
  <UdsPhotoUriWithToken>http://server-name/%%uid%.jpg</UdsPhotoUriWithToken>
</Directory>
```

## OpenLDAP Integration

You can integrate with OpenLDAP using anonymous binds or authenticated binds.

### Anonymous Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using anonymous binds, set the following parameters:

Parameter	Value
<code>BDILDAPServerType</code>	OpenLDAP
<code>BDIPrimaryServerName</code>	IP address Hostname
<code>BDIEnableTLS</code>	True
<code>BDISearchBase1</code>	Root of the directory service or the organizational unit (OU)
<code>BDIServerPort1</code>	The port for the primary directory server
<code>BDIUserAccountName</code>	Unique identifier such as uid or cn

Parameter	Value
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
(Optional) BDIPredictiveSearchFilter	uid or other search filter

The following is an example configuration:

```
<Directory>
  <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>True</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIServerPort1>636/3269</BDIServerPort1>
  <BDIUserAccountName>uid</BDIUserAccountName>
  <BDIBaseFilter>(& (objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

### Authenticated Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using authenticated binds, set the following parameters:

Parameter	Value
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	False
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserAccountName	Unique identifier such as uid or cn
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
(Optional) BDIPredictiveSearchFilter	uid or other search filter
BDIConnectionUsername	Username
BDIConnectionPassword	Password

The following is an example configuration:

```
<Directory>
  <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>False</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIServerPort1>389/3268</BDIServerPort1>
  <BDIUserAccountName>uid</BDIUserAccountName>
  <BDIBaseFilter>(& (objectClass=inetOrgPerson)</BDIBaseFilter>
```

```
<BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>  
<BDIConnectionUsername>cn=administrator,dc=cisco,dc=com</BDIConnectionUsername>  
<BDIConnectionPassword>password</BDIConnectionPassword>  
</Directory>
```

## Federation

Federation lets Cisco Jabber users communicate with users who are provisioned on different systems and who are using client applications other than Cisco Jabber.

## Interdomain Federation

Interdomain federation enables Cisco Jabber users in an enterprise domain to share availability and send instant messages with users in another domain.

- Cisco Jabber users must manually enter contacts from another domain.
- Cisco Jabber supports federation with the following:
  - Microsoft Office Communications Server
  - Microsoft Lync
  - IBM Sametime
  - XMPP standard-based environments such as Google Talk
  - AOL Instant Messenger

You configure interdomain federation for Cisco Jabber on Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. See the appropriate server documentation for more information.

### Related Topics

[Integration Guide for Configuring Cisco Unified Presence Release 8.6 for Interdomain Federation](#)  
[Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager](#)

## Intradomain Federation

Intradomain federation enables users within the same domain to share availability and send instant messages between Cisco Unified Presence and Microsoft Office Communications Server, Microsoft Live Communications Server, or other presence server.

Intradomain federation allows you to migrate users to Cisco Unified Presence or Cisco Unified Communications IM and Presence from a different presence server. For this reason, you configure intradomain federation for Cisco Jabber on the presence server. See the following documents for more information:

- Cisco Unified Presence: *Integration Guide for Configuring Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6 and Microsoft LCS/OCS*
- Cisco Unified Communications IM and Presence: *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*

## Configure Intradomain Federation for BDI or EDI

In addition to configuring intradomain federation on the presence server, you might need to specify some configuration settings in the Cisco Jabber configuration files.

To resolve contacts during contact search or retrieve contact information from your directory, Cisco Jabber requires the contact ID for each user. Cisco Unified Presence uses a specific format for resolving contact information that does not always match the format on other presence servers such as Microsoft Office Communications Server or Microsoft Live Communications Server.

The parameters that you use to configure intradomain federation depend on whether you use *Enhanced Directory Integration (EDI)* or *Basic Directory Integration (BDI)*. EDI uses native Microsoft Windows APIs to retrieve contact data from the directory service and is only used by Cisco Jabber for Windows. For BDI, the client retrieves contact data from the directory service and is used by Cisco Jabber for Mac, Cisco Jabber for Android, and Cisco Jabber for iPhone and iPad.

### Procedure

---

- Step 1** Set the value of the relevant parameter to true:
- For BDI: BDIUseSIPURIToResolveContacts
  - For EDI: UseSIPURIToResolveContacts
- Step 2** Specify an attribute that contains the Cisco Jabber contact ID that the client uses to retrieve contact information. The default value is `msRTCSIP-PrimaryUserAddress`, or you can specify another attribute in the relevant parameter:
- For BDI: BDISipUri
  - For EDI: SipUri
- Note** When you deploy intradomain federation and the client connects with Expressway for Mobile and Remote Access from outside the firewall, contact search is supported only when the contact ID uses one of the following formats:
- `sAMAccountName@domain`
  - `UserPrincipalName (UPN)@domain`
  - `EmailAddress@domain`
  - `employeeNumber@domain`
  - `telephoneNumber@domain`
- Step 3** In the `UriPrefix` parameter, specify any prefix text that precedes each contact ID in the relevant `SipUri` parameter.

#### Example:

For example, you specify `msRTCSIP-PrimaryUserAddress` as the value of `BDISipUri`. In your directory the value of `msRTCSIP-PrimaryUserAddress` for each user has the following format:  
`sip:username@domain`.

- For BDI: BDIUriPrefix

- For EDI: UriPrefix

The following XML snippet provides an example of the resulting configuration for BDI:

```
<Directory>
  <BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts>
  <BDISipUri>non-default-attribute</BDISipUri>
  <BDIUriPrefix>sip:</BDIUriPrefix>
</Directory>
```

The following XML snippet provides an example of the resulting configuration for EDI:

```
<Directory>
  <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
  <SipUri>non-default-attribute</SipUri>
  <UriPrefix>sip:</UriPrefix>
</Directory>
```

## Example of Intradomain Federation

### Intradomain Federation using BDI or EDI

The following example shows how to create intradomain federation contacts using the following BDI or EDI parameters and example values:

#### For BDI: BDISipUri

#### For EDI: SipURI

Value: msRTCSIP-PrimaryUserAddress

#### For BDI: BDIUseSIPURIToResolveContacts

#### For EDI: UseSIPURIToResolveContacts

Value: true

#### For BDI: BDIUriPrefix

#### For EDI: UriPrefix

Value: sip:

For the user Mary Smith, the directory contains sip:msmith@domain.com as the value of the msRTCSIP-PrimaryUserAddress attribute.

The following workflow describes how the client connects to your directory to resolve contact information for Mary Smith:

- 1 Your presence server passes msmith@domain.com to the client.
- 2 The client adds sip: to msmith@domain.com and then queries your directory.
- 3 sip:msmith@domain.com matches the value of the msRTCSIP-PrimaryUserAddress attribute.
- 4 The client retrieves contact information for Mary Smith.

When Cisco Jabber users search for Mary Smith, the client removes the sip: prefix from sip:msmith@domain.com to get her contact ID.