Integrate with Directory Sources

Integrate with Directory Sources for an On-Premises Deployment

Before You Begin

Configure Directory Integration for an On-Premises Deployment.

Procedure

	Command or Action	Purpose
Step 1	Configure Contact Sources, on page 1	
Step 2	Client Configuration for Directory Integration, on page 9	

Configure Contact Sources

The client requires a contact source to search for users and to support contact resolution.

You can configure Enhanced Directory Integration (EDI), Basic Directory Integration (BDI), and Cisco Unified Communications Manager User Data Service (UDS) as contact sources.

Procedure

	Command or Action	Purpose
Step 1	To configure EDI as a contact source, see Domain Name Retrieval, on page 2 and Directory Server Discovery, on page 3.	EDI is an LDAP-based contact source and is the default contact source used by Cisco Jabber for Windows.
Step 2	To configure BDI as a contact source, see Authentication with Contact Sources, on page 3.	BDI is an LDAP-based contact source and is the default contact source used by Cisco Jabber for Mac, iOS, and Android clients.
Step 3	To configure UDS as a contact source, see Enable Integration with UDS, on page 6 and Set UDS Service Parameters, on page 7	Cisco Unified Communications Manager UDS is a Cisco Unified Communications Manager contact source and is available as a contact source for all Cisco Jabber clients. UDS is the contact source used for Expressway Mobile and Remote Access.

Enhanced Directory Integration

Enhanced directory integration (EDI) uses native Microsoft Windows APIs to retrieve contact data from the directory service.

Domain Name Retrieval

Cisco Jabber for Windows retrieves the fully qualified DNS domain from the `USERDNSDOMAIN` environment variable on the client workstation.

After the client gets the DNS domain, it can locate the Domain Name Server and retrieve SRV records.

If the USERDNSDOMAIN environment variable is not present, you can deploy the LdapUserDomain configuration parameter to specify which domain to execute the request for the LDAP service. If that parameter is not configured, then Jabber uses the domain from the email address screen.

In some instances, the value of the `USERDNSDOMAIN` environment variable does not resolve to the DNS domain that corresponds to the domain of the entire forest. For example, when an organization uses a sub-domain or resource domain. In this case, the `USERDNSDOMAIN` environment variable resolves to a child domain, not the parent domain. As a result, the client cannot access information for all users in the organization.

If the `USERDNSDOMAIN` environment variable resolves to a child domain, you can use one of the following options to enable Cisco Jabber for Windows to connect to a service in the parent domain:

- Ensure that the Global Catalog or LDAP directory server can access all users in the organization.
- Configure your DNS server to direct the client to a server that can access all users in the organization when Cisco Jabber for Windows requests a Global Catalog or LDAP directory server.
- Configure Cisco Jabber for Windows to use the FQDN of the domain controller.

  Specify the FQDN of the domain controller as the value of the PrimaryServerName parameter in your client configuration as follows:
  `<PrimaryServerName>`*`parent-domain-fqdn`*`</PrimaryServerName>`

Related Topics

Configuring DNS for the Forest Root Domain
Assigning the Forest Root Domain Name
Deploying a GlobalNames Zone
Support for DNS Namespace planning in Microsoft server products

Directory Server Discovery

Cisco Jabber can automatically discover and connect to the directory server if:

- The workstation on which you install Cisco Jabber automatically detects the workstation by determining the user domain.
- The workstation retrieves the server connection address from the DNS SRV record.

Directory Server	SRV Record
Global Catalog	`_gc._msdcs._tcp.`*`domain.com`*
Domain Controller LDAP-based directory servers	`_ldap._msdcs._tcp.`*`domain.com`*

Basic Directory Integration

BDI is an LDAP-based contact source and is the default contact source used by Cisco Jabber for Mac, iOS, and Android clients.

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 — 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.

Use a well-known or public set of credentials for 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 release 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.

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.

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 release 9.x and later, 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 Select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 3 Select **Add New**.
The **UC Service Configuration** window opens.

Step 4 In the **Add a UC Service** section, select **Directory** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Enter details for the directory service:

- Product Type — Select **Directory**

- Name — Enter a unique name for the directory service
- Hostname/IP Address — Enter the Hostname, IP Address, or FQDN of the directory server.
- Protocol Type — From the drop-down list, select:
  - TCP or UDP for Cisco Jabber for Windows
  - TCP or TLS for Cisco Jabber for iPhone or iPad
  - TCP or TLS for Cisco Jabber for Android

- Product Type — Select **Directory**
- Name — Enter a unique name for the directory service
- Hostname/IP Address — Enter the Hostname, IP Address, or FQDN of the directory server.
- Protocol Type — From the drop-down list, select:
  - TLS if you want Cisco Jabber to connect to the Directory by using TLS.
  - TCP if you want Cisco Jabber to connect to the Directory by using TCP.

Step 7 Select **Save**.

Step 8 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 **Primary**, **Secondary**, and **Tertiary** drop-down lists:

d) Specify the **Username** and **Password** that the client can use to authenticate with the LDAP server in the following fields:

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.

Use a well-known or public set of credentials for 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
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>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

Cisco Unified Communications Manager User Data Service

User Data Service (UDS) is a REST interface on Cisco Unified Communications Manager that provides contact resolution.

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 server to ensure that the client can discover the server.
The following is an example configuration for the Cisco Unified Communications Manager server:
```
<UdsServer>11.22.33.444</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
Enable All User Search	Allows searches for all users in the directory (search with no last name, first name, or directory number specified). The default value is true.
User Search Limit	Limits the number of users returned in a query. The default value is 64.
Number of Digits to Match	Specifies the number of digits to match when users search for phone numbers. **Tip** To resolve PSTN numbers, set the value 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, synchronize all users on the corporate directory to each cluster. 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, synchronize all 40,000 users to both clusters. 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`.

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.

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 Communications Manager IM & Presence server 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
- UserPrincipleName (UPN)@domain
- EmailAddress@domain
- employeeNumber@domain
- phoneNumber@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 SipUri. 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>
```

Client Configuration for Directory Integration

You can configure directory integration through service profiles using Cisco Unified Communications Manager release 9 or later or with the configuration file. Use this section to learn how to configure the client for directory integration.

When both a service profile and a configuration file are present, the following table describes which parameter value takes precedence.

Service Profile	Configuration File	Which Parameter Value Takes Precedence?
Parameter value is set	Parameter value is set	Service profile
Parameter value is set	Parameter value is blank	Service profile
Parameter value is blank	Parameter value is set	Configuration file
Parameter value is blank	Parameter value is blank	Service profile blank (default) value

Note Cisco Unified Presence, Release 8.x profiles cannot be used for directory integration.

Configure Directory Integration in a Service Profile

With Cisco Unified Communications Manager release 9 and later, you can provision users with service profiles and deploy the `_cisco-uds` SRV record on your internal domain server. The client can then automatically discover Cisco Unified Communications Manager and retrieve the service profile to get directory integration configuration.

Procedure

	Command or Action	Purpose
Step 1	Add a Directory Service, on page 10	Create a Directory UC Service.
Step 2	Apply Directory Service to a Service Profile, on page 14	Add the Directory UC Service to the Service Profile.

Add a Directory Service

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 3 Select **Add New**.
The **UC Service Configuration** window opens.

Step 4 Select **Directory** from the **UC Service Type** menu and then select **Next**.

Step 5 Set all appropriate values for the directory service.

To configure Cisco Jabber directory searches on the Global Catalog, add the following values:

- **Port—**3268
- **Protocol—**TCP

Step 6 Select **Save**.

What to Do Next

Apply Directory Service.

Directory Profile Parameters

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

Directory Service Configuration	Description
Primary server	Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.
Secondary server	Specifies the address of the backup directory server.
Tertiary Server	Applies to Cisco Jabber for Windows only. Specifies the address of the tertiary directory server.
Use UDS for Contact Resolution	Specifies if the client uses UDS as a contact source. **True (Default)** Use UDS as a contact source. When this option is selected the following parameters in this table are not used. **False** Use EDI or BDI as a contact source. The following parameters are used to connect to the LDAP server. By default, UDS provides contact resolution when users connect to the corporate network through Expressway for Mobile and Remote Access.

Directory Service Configuration	Description
Use Logged On User Credential	Specifies if the client uses the logged on username and password for LDAP contact resolution. If you have configured Active Directory (AD) SSO, this will take priority over this setting. **True (default)** Use logged on user credentials. This value maps to the values for the UseWindowsCredentials parameter for Windows clients, and the BDIUseJabberCredntials parameter for other clients. **False** Do not use logged on user credentials. When you have SSO configured, Jabber uses those credentials before using the ConnectionUsername and ConnectionPassword parameters. You must specify the logged on user credentials with the following parameters: • ConnectionUsername • ConnectionPassword You must specify the logged on user credentials with the following parameters: • EDI (Windows client) ◦ ConnectionUsername ◦ ConnectionPassword • BDI (Mac, Android, iOS clients) ◦ BDIConnectionUsername ◦ BDIConnectionPassword
Username	Lets you manually specify a shared username that the client can use to authenticate with the directory server. By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials. Use only a well-known or public set of credentials for an account that has read-only permissions.

Directory Service Configuration	Description
Password	Lets you manually specify a shared password that the client can use to authenticate with the directory server. By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials. Use only a well-known or public set of credentials for an account that has read-only permissions.
Search Base 1 The following parameters only apply to Cisco Jabber for Windows: **Search Base 2** **Search Base 3**	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. 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. Active Directory does not typically require a search base. Specify search bases for Active Directory only for specific performance requirements. Specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory. **Tip** 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.
Recursive Search on All Search Bases	Select this option to perform a recursive search of the directory starting at the search base. Use recursive searches to allow the Cisco Jabber client contact search queries to search all of the LDAP directory tree from a given search context (search base). This is a common option when searching LDAP. This is a required field. The default value is True.
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 `(&(&(objectCategory=person)(objectClass=user)`.

Directory Service Configuration	Description
Predictive Search Filter	Defines filters to apply to predictive search queries. You can define multiple, comma-separated values to filter search queries. The default value is `ANR`. When Cisco Jabber performs a predictive search, it issues a query using Ambiguous Name Resolution (ANR). This query disambiguates the search string and returns results that match the attributes that are set for ANR on your directory server. **Important** Configure your directory server to set attributes for ANR if you want the client to search for those attributes.

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.

Apply Directory Service to a Service Profile

Procedure

Step 1 Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.

Step 2 Select **Add New**.
The **Service Profile Configuration** window opens.

Step 3 Add the directory services to the directory profile. See the *Directory Profile Parameters* topic for information about the specific settings that are needed for the directory profile.

Step 4 Select **Save**.

Advanced Directory Integration in the Configuration File

You can configure directory integration in the Cisco Jabber configuration file. For more information see the *Directory* chapter in the *Parameters Reference Guide for Cisco Jabber*.

Important When a Service Profile and a configuration file are present, settings in the Service Profile always take priority.