Installing the Cisco Unified CallManager Customer Directory Plugin Release 4.3(1)

Cisco Unified CallManager uses a Lightweight Directory Access Protocol (LDAP) directory to store data as well as authentication and authorization information about users of Cisco Unified CallManager applications, which interface with the Cisco Unified CallManager. Authentication establishes the user right to access the system, while authorization identifies the telephony resources that a user is permitted to use, such as a specific telephone extension. Cisco Unified CallManager stores the following data in the LDAP directory:

- Application-specific profiles for users (for example, the devices that are associated to a user, whether the devices are enabled to use CTI applications, and so on)
- Information for the Personal Directory services, Personal Address Book, and Personal Fast Dials
- Authentication information for Cisco Unified CallManager Multilevel Administration (MLA)
- User information from the User Information window in Cisco Unified CallManager Administration

Cisco Unified CallManager uses Data Connection Directory (DC-Directory) as an embedded LDAP directory. The Cisco Customer Directory Plugin allows you to integrate Cisco Unified CallManager with one of the following enterprise directories:

- Microsoft Active Directory (AD), available with Microsoft Windows 2000
- Microsoft Active Directory (AD 2003), available with Microsoft Windows 2003
- Netscape Directory Server (Version 4.x), iPlanet Directory Server (Version 5.1), and Sun ONE Directory Server (Version 5.2)

After the LDAP directory configuration completes, you can use the Corporate Directory service on your Cisco Unified IP Phones 7940, 7960, and 7970 to look up users in the enterprise directory. You can also upload completed workflow application files to the directory. The application server downloads the files to run workflow applications when you use the administration client to start a specific application.

Note You can configure the Corporate Directory service on the Cisco Unified IP Phone to access an enterprise directory without integrating Cisco Unified CallManager. For information on integrating only the Corporate Directory service with the Cisco Unified IP Phone, refer to the documentation that is included within the IP Phone Services software development kit (SDK) that is available on cisco.com.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Cisco Customer Directory Configuration Plugin Overview

You use the Cisco Customer Directory Configuration Plugin only if you want to integrate Cisco Unified CallManager with your enterprise directory, and you do not want to use the embedded DC-Directory. This plug-in, which includes support for Netscape Directory Server and Microsoft Active Directory, installs only on servers that are running Cisco CallManager 3.0(10) or later. Starting with the publisher database server, you install the plug-in on all Cisco Unified CallManager servers in the cluster. On the publisher database server, the plug-in installs the schema, configures the directory, and integrates Cisco Unified CallManager with the directory. On the subscriber servers, the plug-in only integrates Cisco Unified CallManager with the directory.

You must have a directory account with rights to extend the schema. For more information on obtaining these rights and for installation and configuration assistance, contact your Netscape Directory Server or Microsoft Active Directory administrator.

Caution Microsoft Active Directory does not support schema deletion. After you have installed the Cisco schema extensions, you cannot revert to the previous schema. Cisco recommends that you back up your Microsoft Active Directory server, especially the schema master, before you install/configure the Cisco Customer Directory Configuration Plugin and install the Cisco schema extensions on your Microsoft Active Directory server. For information on backing up your Microsoft Active Directory server, contact your Microsoft Active Directory administrator.

Caution Using non-ISO-Latin1 characters greater than 127 with DC Directory, Netscape Directory, or Active Directory can cause directory database errors. Cisco Unified CallManager Release 4.2(2) supports all ISO-Latin1 (ISO-8859-1) characters and all non-ISO-Latin1 characters in the range 0-127 with any directory. Cisco Unified CallManager only supports ISO-Latin1 and ASCII characters in the User area of Cisco Unified CallManager Administration. After you download the locale installer, you can display field names in the User area of Cisco Unified CallManager Administration in your chosen language. However, Cisco Unified CallManager only supports ISO-Latin1 (ISO-8859-1) characters and non-ISO-Latin1 characters in the range 0-127 in the fields and in all user accounts and passwords that are needed to access these windows. If a user enters data that is not in the allowed character range, a dialog box displays and states that the user must enter data by using only ISO-Latin1 characters and non-ISO-Latin1 characters in the range 0-127. CDR Analysis and Reporting (CAR) supports all ISO-Latin1 (ISO-8859-1) characters and non-ISO-Latin1 characters in the range 0-127.

Integrating the Directory After a Cisco Unified CallManager Installation or Upgrade

You use the Cisco Customer Directory Configuration Plugin only if you want to integrate the Cisco Unified CallManager with your enterprise directory, and you do not want to use the embedded DC-Directory. After you complete the Cisco Unified CallManager installation or upgrade on every server in the cluster, you install or upgrade the plug-in; always install the plug-in on the publisher database server before you install it on the subscriber servers. For more information on the order for installing the plug-in, see Table 1 on page 5.

Note If you upgrade Cisco Unified CallManager after you integrate your enterprise directory with Cisco Unified CallManager, you must reinstall the Cisco Customer Directory Configuration Plugin on each server in the cluster by using Table 1 on page 5, the installation section, and the appropriate integration sections as a guide. After a Cisco Unified CallManager upgrade, reinstalling the plug-in populates your enterprise directory with any additional schema extensions and data entries that version of Cisco Unified CallManager needs.

Caution Do not use Terminal Services to install or upgrade the plug-in. Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote management and troubleshooting tasks. You can use Virtual Network Computing (VNC) to install the plug-in, but be aware that VNC may cause high CPU usage in your network. For more information on using VNC, click the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/vnc/index.htm

Password Management Features

The following enterprise directories can provide password management features after they are integrated with the Cisco Unified CallManager:

- Microsoft Active Directory (AD), available with Microsoft Windows 2000
- Microsoft Active Directory (AD 2003), available with Microsoft Windows 2003
- Netscape Directory Server (Version 4.x), iPlanet Directory Server (Version 5.1), and Sun ONE Directory Server (Version 5.2)

Note The Cisco Unified CallManager embedded DC-Directory does not support password management features.

You can configure password management features for Cisco Unified CallManager (LDAP) users, and, if MLA is enabled, for administrative users. You can configure the following password management features:

- Require users to change their passwords when they access their accounts for the first time after creation or after the administrator has reset the password.
- Require users to create strong passwords by adhering to configurable length and complexity rules.
- Require users to change their passwords after a configurable time.

Refer to your enterprise directory documentation for password management configuration procedures.

Note Cisco Unified CallManager cannot notify users that their passwords are about to expire. If a password expires, the user cannot log in to Cisco Unified CallManager User Options to change it and must request a password reset from the enterprise directory administrator. Cisco recommends that you take this into consideration when you are communicating password management requirements to users.

Caution To prevent disruption of critical access to the system, never configure a password expiration time for the following system users: CCMAdministrator, CCMSysUser, IPMASysUser, and any other system user that any Cisco Unified CallManager application creates and uses. You must set passwords for these users to never expire.

Plug-in Installation Procedure

To install the plug-in after a Cisco Unified CallManager installation or upgrade, perform the tasks in the order that is specified in Table 1:

Table 1 Order for Installing Plug-in

Task		Related Information
Step 1	Verify that you completed the Cisco Unified CallManager installation/upgrade on every server in the cluster.	Refer to the Cisco Unified CallManager installation and upgrade documentation that matches this version of the plug-in.
Step 2	On the publisher database server, disable and stop all Cisco-approved, third-party applications and Cisco-supported applications, such as Cisco Security Agent, McAfee antivirus services, Prognosis, and so on, if these applications are installed.	Refer to the documentation that supports the application that you want to disable.
Step 3	On the publisher database server, install the Cisco Customer Directory Configuration Plugin.	• Installing the Cisco Customer Directory Configuration Plugin, page 7 • Integrating Netscape Directory Server, iPlanet Directory Server, or Sun ONE Directory Server with Cisco Unified CallManager, page 9 • Integrating Microsoft Active Directory with Cisco Unified CallManager, page 12
Step 4	On the publisher database server only, run the CCMPWDChanger tool to change the passwords for CCMSysUser, CCMAdministrator, and IPMASysUser. This step applies only to Active Directory.	Enabling Cisco IP Services After Directory Integration on the Publisher Database Server (Required), page 23 **Caution** Before you install the Cisco Customer Directory Configuration Plugin on subscriber servers, you must perform the procedure in "Enabling Cisco IP Services After Directory Integration on the Publisher Database Server (Required)" section on page 23. If you attempt to install the plug-in on the subscriber servers before you perform the service integration procedure, the installation displays a message, and the Cisco Extended Functions, Cisco IP Manager Assistant, and Cisco CallManager Extension Mobility services do not function.

Table 1 Order for Installing Plug-in (Continued)

Task		Related Information
Step 5	**Note** You must perform this mandatory step after plug-in installation. On the publisher database server, configure MLA to move all users and user groups to the new directory. Make sure that the MLA window displays without errors. If you are installing the plug-in on subscriber servers, perform this step on the subscriber servers.	Installing the Cisco Customer Directory Configuration Plugin, page 7, Step 9 and Step 10.
Step 6	On the publisher database server only, run an LDAP Data Interchange Format (LDIF) tool to process the data and update the directory. One such tool, **ldapmodify.exe**, exists on the server to import the data from the LDIF file to the directory. If you want to use a different tool to import the data, you may do so.	Importing Data from the LDIF Files to the Enterprise Directory, page 24 You must perform Step 6 when you choose only the Generate Configuration LDIF Files option (Custom mode). You do not need to perform Step 6 under the following circumstances: • If you choose the Express mode. • If you do not choose the Generate Configuration LDIF Files option (Custom mode).
Step 7	After you run the CCMPWDChanger tool and change the appropriate passwords (see Step 4), enable all Cisco-approved, third-party applications and Cisco-supported applications on the publisher database server.	Refer to the documentation that supports the application that you want to enable.
Step 8	On the subscriber servers, disable and stop all Cisco-approved, third-party applications and Cisco-supported applications, such as Cisco Security Agent, McAfee antivirus services, Prognosis, and so on, if these applications are installed.	Refer to the documentation that supports the application that you want to disable.

Table 1 Order for Installing Plug-in (Continued)

Task		Related Information
Step 9	On the subscriber servers, install the Cisco Customer Directory Configuration Plugin. Enter the host name and port number of the directory server. The value that is read from the publisher prepopulates the host name and port number. On the subscriber server, you can change the host name and port number, so the load balancing can be done by pointing to an alternate server that has the data replicated from the server to which the publisher is integrated. You may also enable or disable SSL. **Tip** After you verify that you installed the plug-in and changed the passwords on the publisher database server, you can install the plug-in on all subscriber servers simultaneously.	• Installing the Cisco Customer Directory Configuration Plugin, page 7 • Integrating Netscape Directory Server, iPlanet Directory Server, or Sun ONE Directory Server with Cisco Unified CallManager, page 9 • Integrating Microsoft Active Directory with Cisco Unified CallManager, page 12
Step 10	After you install the Cisco Customer Directory Configuration Plugin on the subscriber servers, enable the Cisco-approved, third-party applications and Cisco-supported applications.	Refer to the documentation that supports the application that you want to enable.
Step 11	Restore applications that used DC-Directory.	Restoring Applications After Directory Integration (Required If Application Is Installed), page 26

Installing the Cisco Customer Directory Configuration Plugin

Perform the following steps to install the Cisco Customer Directory Configuration Plugin:

Step 1 Starting with the publisher server, choose **Start > Programs > Cisco Unified CallManager > Cisco Unified CallManager Administration** and log in with system administrative privileges.

Step 2 Choose **Application > Install Plugins**.

Step 3 Click the plug-in icon for **Cisco Customer Directory Configuration**.

Step 4 Download the plug-in to the desktop.

Step 5 Double-click the **Cisco Customer Directory Configuration Plugin** icon that displays on the desktop.

Step 6 A prompt may ask you to verify whether the host server acts as the publisher or subscriber server. If you already integrated Cisco Unified CallManager with an enterprise directory, the plug-in does not display this prompt. If the host server acts as a subscriber, a prompt asks you for authentication to the publisher server. Enter the Windows 2000 user name and password with local administrative rights on the publisher server.

Cisco requires authentication to the publisher database server, so certain fields automatically populate during the configuration process. You must enter the publisher password during the subscriber server installation, or the plug-in automatically terminates the installation.

The plug-in also tries to retrieve the userid and encrypted password of the Cisco Unified CallManager system users (CCMSysUser, CCMAdministrator, and IPMASysUser) from the publisher registry. If the plug-in cannot retrieve these userids and passwords, a warning message displays with a field where you can set the passwords on the publisher server. If you click **OK** without entering the system user passwords and the plug-in cannot retrieve the system user passwords from the publisher server, a second warning message displays to indicate that the plug-in could not retrieve the password. The installation continues, but you must set these passwords after the installation by using the procedure that is described in "Enabling Cisco IP Services After Directory Integration on the Publisher Database Server (Required)" section on page 23.

Step 7 In the Components window, you may see one or more of the following options. From the window, check one of the following options:

- If you check **Configure Netscape Directory Server** (or **Upgrade Netscape Directory Configuration**), go to the "Integrating Netscape Directory Server, iPlanet Directory Server, or Sun ONE Directory Server with Cisco Unified CallManager" section on page 9.

Note Check the **Configure Netscape Directory Server** option for iPlanet Directory Server and Sun ONE Directory Server.

- If you check **Configure Active Directory Server** (or **Upgrade Microsoft Active Directory Configuration**), go to the "Integrating Microsoft Active Directory with Cisco Unified CallManager" section on page 12.

Note If you check Uninstall Active Directory Configuration (or Uninstall Netscape Directory Configuration), which is available after an initial installation, Cisco Unified CallManager automatically integrates with DC-Directory.

Step 8 To return to the Cisco Unified CallManager application, choose **Start > Programs > Cisco Unified CallManager > Cisco Unified CallManager Administration**.

Step 9 To configure the MLA enterprise parameters, choose **User > Access Rights > Configure MLA Parameters**.

Make sure that the MLA Enterprise Parameter Configuration window displays without errors. See Table 2 for an example of the information that displays.

Table 2 MLA Enterprise Parameters

Parameter Name	Parameter Value
User Group Base	ou=MultiLevelAdmin,ou=Admins,o=cisco.com
Administrative User Base	ou=Users,o=cisco.com
Debug Level	None
Effective Access Privileges For Overlapping User Groups	Maximum
Effective Access Privileges For Overlapping Functional Groups	Maximum
Enable MultiLevelAdmin	False
User Cache Flush Timeout (Minutes)	5

Note If you change the value of the Enable MultiLevelAdmin or User Cache Flush Timeout (Minutes) parameter, a message displays that prompts you to restart the web server in all Cisco Unified CallManager systems in the cluster for the change to take effect.

For more information on MLA enterprise parameters, refer to the *Cisco Unified CallManager System Guide* and the *Cisco Unified CallManager Administration Guide*.

Step 10 If the MLA Enterprise Parameter Configuration window displays errors, perform the following steps:

a. Access the trace files in the MLA trace directory (C:\program files\cisco\traces\MLA).

b. Look for the information DirAndUInn.txt (where nn=01, 02, 03 ...) and Permissions0000000nn.txt (where nn=01, 02, 03 ...).

c. Save the trace file (for debugging purposes).

d. Stop IIS Admin Services by choosing **Start > Administrative Tools > Services**.

e. Start IIS Admin and World Wide Web Publishing Services.

Integrating Netscape Directory Server, iPlanet Directory Server, or Sun ONE Directory Server with Cisco Unified CallManager

Perform the following steps to configure the Netscape Directory Server, iPlanet Directory Server, or Sun ONE Directory Server.

Note Although many of the fields specify Netscape Directory Server, follow the same procedure for iPlanet Directory Server and Sun ONE Directory Server.

Step 1 You may receive a prompt with one of the following two configuration options:

a. Check **Express** if you want the plug-in to configure the directory and enable Cisco Unified CallManager integration with the directory. On the publisher server, the plug-in creates Cisco-specific containers and objects and updates the configuration settings on the Cisco Unified CallManager server to point to the directory server. During the configuration process, the installation program also enables you to extend the schema. On the subscriber server, the plug-in updates the configuration settings and presents a configuration window for security (LDAP over SSL). Click **Next** and go to Step 3.

Note Cisco recommends that you check the Express option. Cisco makes the Custom option available for administrators who are experienced with Netscape Directory Server, iPlanet Directory Server, or Sun ONE Directory Server. Only the publisher server can access the Express and Custom options.

b. To choose the installation options separately, check **Custom**. Click **Next** and continue.

Step 2 Check all the following check boxes that apply. If you want to do so, you can click the **Select All** button. After you finish making your choices, click **Next**.

- Configure Netscape Directory—Adds Cisco-specific containers and objects and allows you to extend the schema.
- Enable Cisco Unified CallManager Integration with Netscape Directory—Updates the configuration settings on the Cisco Unified CallManager server to point to the directory server.
- Generate Configuration LDIF Files—Generates LDIF files for directory configuration. If you want to generate the LDIF files without performing the operations on the directory server, choose only this option (not the other options in the window). For more information on LDIF files and for additional tasks that you must perform, see the "Importing Data from the LDIF Files to the Enterprise Directory" section on page 24.

Caution Choosing only the Generate Configuration LDIF Files option does not integrate your enterprise directory; if you choose only the Generate Configuration LDIF Files option and fail to choose the other options, you must run the plug-in again on all servers in the cluster and choose only the Enable Cisco Unified CallManager Integration with Netscape Directory option after you import the LDIF files to the enterprise directory.

Step 3 The Customer Information window prompts you for the following information, as seen in Table 3 on page 10. Most fields in this window display prepopulated information. Verify that this information is correct before continuing the configuration process.

Note On the subscriber servers, the prepopulated information comes from the publisher database server, and you can edit only the Host Name and Port Number fields.

Table 3 Customer Information Window

Field	Recommended Action
Host Name	Enter the hostname (or IP address) where you installed the enterprise directory.
Port Number	Enter the port number on which the enterprise directory receives the LDAP requests.
Directory Administrator DN	Enter the enterprise directory Directory Administrator Distinguished Name (DN). The Directory Administrator DN that you enter in this field must have the rights to update the enterprise directory schema. Typically, the users who have the rights to update the schema belong to the *Schema Admin* group. Contact your enterprise directory administrator for information on users who can update the schema.
Directory Administrator Password	Enter the enterprise directory password.
Confirm Password	Enter the enterprise directory password again.

Table 3 Customer Information Window (Continued)

Field	Recommended Action
Cisco Directory Configuration DN	Enter the Cisco Directory Configuration Distinguished Name. This field specifies the DN where the Cisco-dependent schema is created for the Cisco Unified CallManager.
User Search Base	Enter the User Search Base. Cisco Unified CallManager searches for users under this base.
User Creation Base	Enter the User Creation Base. Any user that is created by using Cisco Unified CallManager Administration resides under this node in the directory. **Note** Make the User Creation Base the same as the User Search Base or a subtree under the User Search Base. If you do not, you cannot look up users that you create in Cisco Unified CallManager Administration.
User Naming Attribute	Enter the Relative Distinguished Name (RDN) for user entries. Examples include **cn**, **uid**, and so forth.
User Search Attribute	Enter an attribute that you can use to search for a user in the enterprise directory. Make sure that the value for this attribute is unique for each user in the directory. Examples include **mail** or **uid**. **Note** The user enters the value for this attribute in the User Identification field when the user logs in to the Cisco Unified IP Phone User Option window.

Step 4 After you enter the information into the fields, click the **Next** button.

Step 5 The Configure LDAP over SSL dialog box displays. If you want security implemented, check the Enable LDAP over SSL check box; otherwise, click the **Next** button and continue with Step 9.

Step 6 If you checked the Enable LDAP over SSL check box, enter the SSL port number.

Step 7 To continue the security configuration process, you must copy the certificate of CA that has issued the SSL certificate that is installed on the directory server to the publisher server. You need to enter this certificate filename in the text box next to the **Browse** button (or use the **Browse** button to find the copy of the file that is on the publisher server).

Note The first time that security is configured, copy the certificate to the publisher server and specify the path to that file in the text box that is on the Configure LDAP over SSL window. If this is an upgrade and SSL is already enabled, copy the certificate file and specify the path only if the certificate changed since the previous installation/upgrade.

If you click **Browse**, a new window opens that allows you to find the certificate file that needs to be selected.

Step 8 Click the **Next** button. The system begins to verify whether you entered the configuration information correctly.

Step 9 If you entered the information correctly, a confirmation window summarizes the configuration information. Click the **Next** button.

Note If you did not enter the information correctly, a message displays and prompts you to enter the correct information.

Step 10 Click the **FINISH** button and reboot your server (required).

Integrating Microsoft Active Directory with Cisco Unified CallManager

Cisco recommends that Cisco Unified CallManager and Active Directory use the same Domain Name Service (DNS) server. If you cannot use the same DNS server, you must provide the name to IP address mapping for all the Active Directory (AD) servers in your AD forest in the hosts file or use another DNS server that can resolve the names of all the AD servers in your AD forest.

Cisco supports the integration of multiple Cisco Unified CallManager clusters with the same Microsoft Windows Active Directory (AD) forest with the following caveats:

- Because of the complex nature of a large number of potential combinations of customer AD configurations and Cisco voice applications that can be deployed together with Cisco Unified CallManager and that also use the directory, you must adhere to specific guidelines.
- Before you proceed with a multicluster integration, you must contact your local Cisco sales team to initiate a request for this specific support.
- When you deploy other Cisco voice applications in addition to Cisco Unified CallManager, including CAR, MLA, Cisco IP Contact Center (IPCC), and Cisco Unified Contact Center Express, additional limitations may apply. For additional information, refer to the applicable documentation and release notes for your specific product.

Perform the following procedure to integrate Cisco Unified CallManager with Microsoft Active Directory:

Step 1 If you checked **Configure Active Directory Server** (or **Upgrade Active Directory Configuration**), a prompt asks you to check either Express or Custom, which are setup options that are available only to the publisher server. Check the appropriate check box and see the following steps, depending on which option you choose:

- For Express Option, see Step 2.
- For Custom Option, see Step 12.
- For subscribers, see Step 3

Express Option

Cisco recommends that you check the Express option. Cisco makes the Custom option available for administrators who are experienced with Microsoft Active Directory.

Step 2 If you checked **Express**, the plug-in configures Active Directory and enables Cisco Unified CallManager integration with Active Directory. On the publisher server, the plug-in updates the schema, creates Cisco-specific objects and containers, and updates the configuration settings on the Cisco Unified CallManager server to point to AD server. Click the **Next** button and go to Step 3.

Step 3 A prompt asks you for the Microsoft Active Directory server host name and port number. Cisco Unified CallManager prepopulates the fields if the values exist in the registry.

a. In the Host Name field, enter the Hostname (or IP address) of the Active Directory Schema Master server.

b. In the Port Number field, enter the port number where Microsoft Active Directory receives the LDAP requests. The default specifies 389.

Step 4 If you are configuring a subscriber server and you want to configure security (LDAP over SSL), go to Step 7. If you do not want security, go to Step 26; otherwise, click **Next** and continue.

Step 5 On the publisher database server, the plug-in obtains the domain name in the Microsoft Active Directory server. In the Active Directory Configuration window, you may see the following information from Table 4 on page 13 prepopulated in the fields. Verify the information before continuing the configuration process.

Table 4 Active Directory Configuration Window

Field	Recommended Action
Directory Administrator DN	Enter the Microsoft Active Directory Administrator Distinguished Name. The Directory Administrator DN that you enter in this field must have the rights to update the Active Directory schema. Typically, the users who have the rights to update the schema belong to the *Schema Admin* group. Contact your Active Directory administrator for information on users who can update the schema.
Directory Administrator Password	Enter the password for the Directory Administrator DN user.
Confirm Password	Enter the password again.
Cisco Directory Configuration DN	Enter the Cisco Directory Configuration Distinguished Name. This field specifies the DN where the Cisco-dependent schema is created for the Cisco Unified CallManager.
User Search Base	Enter the User Search Base. Cisco Unified CallManager searches for users under this base.
User Creation Base	Enter the User Creation Base. Any user that is created by using Cisco Unified CallManager Administration resides under this node in the directory. **Note** Make the User Creation Base the same as the User Search Base or a subtree under the User Search Base. If you do not, you cannot look up users that you create in Cisco Unified CallManager Administration.

Table 4 Active Directory Configuration Window (Continued)

Field	Recommended Action
User Search Attribute	Enter an attribute that you can use to search for a user in the enterprise directory. Make sure that the value for this attribute is unique for each user in the directory. Examples include **mail** or **uid**. **Note** When the user logs in to the Cisco Unified IP Phone User Options window, the user enters the value for this attribute in the User Identification field.
Domain Name	Enter the Microsoft Active Directory domain name. This domain name represents the schema master.

Step 6 If you are satisfied with the Active Directory configuration information, click **Next**.

Step 7 The Configure LDAP over SSL dialog box displays. If you want security implemented, check the Enable LDAP over SSL check box; otherwise, click the **Next** button and continue with Step 11.

Step 8 If you checked the Enable LDAP over SSL check box, enter the SSL port number (the default port number specifies 636).

Step 9 To continue the security configuration process, you must copy the certificate of CA that has issued the SSL certificate that is installed on the directory server to the publisher server. You must enter this certificate filename in the text box next to the **Browse** button (or use the **Browse** button to find the copy of the file that is on the publisher server).

Note The first time that security is configured, copy the certificate to the publisher server and specify the path to that file in the text box that is on the Configure LDAP over SSL window. If this is an upgrade and SSL is already enabled, copy the certificate file and specify the path only if the certificate changed since the previous installation/upgrade.

If you click **Browse**, a new window opens that allows you to find the certificate file that needs to be selected.

Step 10 Click the **Next** button. The system begins to verify whether you entered the configuration information correctly.

Step 11 On the publisher database server, the plug-in installs the schema, configures the Microsoft Active Directory, and integrates Cisco Unified CallManager with the Microsoft Active Directory. On the subscriber server, the plug-in only integrates Cisco Unified CallManager with this Microsoft Active Directory. To complete the Express configuration, go to Step 26.

Custom Option

Step 12 If you checked **Custom**, nonexclusive custom installation options display in the window. You may check as many of the check boxes as you want. If you want all the options, click the **Select All** button. After you finish making your choices, click the **Next** button.

- Install Schema on Schema Master—Installs schema updates.
- Configure Active Directory—Adds Cisco-specific containers and objects and allows you to extend the schema.

- Enable Cisco Unified CallManager Integration with Active Directory—Updates the configuration settings on the Cisco Unified CallManager server to point to the Active Directory server.
- Generate Configuration LDIF Files—Generates LDIF files, which contain LDAP data in flat files, for schema updates and enterprise directory configuration. For more information on LDIF files and for additional tasks that you must perform, see the "Importing Data from the LDIF Files to the Enterprise Directory" section on page 24.

Caution Choosing only the Generate Configuration LDIF Files option does not integrate your enterprise directory; if you choose only the Generate Configuration LDIF Files option and fail to choose the other options, you must run the plug-in again on all servers in the cluster and choose only the Enable Cisco Unified CallManager Integration with Active Directory option after you import the LDIF files to the enterprise directory.

Step 13 See the following steps, depending on the options that you chose:

- For Install Schema on Schema Master, Generate Configuration LDIF Files, or Select All, go to Step 14.
- For Enable Cisco Unified CallManager Integration with Active Directory, go to Step 18.
- For Configure Active Directory, go to Step 19.

Caution Microsoft Active Directory does not support schema deletion. After you have installed the Cisco schema extensions, you cannot revert to the old schema. Cisco recommends that you back up your Microsoft Active Directory server, especially the schema master, before you install/configure the Cisco Customer Directory Configuration Plugin and install the Cisco schema extensions on your Microsoft Active Directory server. For more information on backing up your Microsoft Active Directory server, contact your Microsoft Active Directory administrator.

Step 14 If you checked Install Schema on Schema Master or Select All, a dialog box may state that Active Directory does not support schema deletion; if this dialog box displays, click **OK**.

Step 15 If you checked Install Schema on Schema Master, Generate Configuration LDIF Files, or Select All, the Customer Information window opens, so you can enter the schema master host name and port number, if the window is not already prepopulated with the correct information.

Step 16 The plug-in retrieves the domain name from the schema master and prepopulates the following information, as listed inTable 5. Verify the information before continuing the configuration process.

Table 5 Active Directory Configuration Window

Field	Recommended Action
Directory Administrator DN	Enter the Microsoft Active Directory Administrator Distinguished Name. The Directory Administrator DN that you enter in this field must have the rights to update the Active Directory Schema. Typically, the users who have the rights to update the schema belong to the *Schema Admin* group. Contact your Active Directory administrator for information on users who can update the schema.
Directory Administrator Password	Enter the password for the Directory Administrator DN user.
Confirm Password	Enter the password again.
Domain Name	Enter the Microsoft Active Directory domain name.
Credential to configure Active Directory same as above	This check box may display if you checked the Configure Active Directory, the Enable CallManager Integration with Active Directory, or the Generate Configuration LDIF Files check boxes during the Custom configuration. Checking this check box ensures that the information in Step 18 and Step 19 prepopulates.

The plug-in installs the schema on the schema master, according to the information that you previously entered or verified.

Step 17 Click **Next** and continue the configuration process.

Step 18 If you checked Configure Active Directory or Enable Cisco Unified CallManager Integration with Active Directory and not Install Schema on the Schema Master, enter the Microsoft Active Directory server host name and port number. Click the **Next** button.

Step 19 The plug-in retrieves the domain name from the Microsoft Active Directory server and may prepopulate the following information, as shown in Table 6. Verify the information before continuing the configuration process.

Table 6 Active Directory Configuration Window

Field	Recommended Action
Directory Administrator DN	Enter the Microsoft Active Directory Administrator Distinguished Name. You can enter the same Directory Administrator DN that you entered in Step 16. The user that you entered in Step 16 serves as a schema administrator. If you do not want to use the schema administrator, you can create another user, such as dcd admin, in Active Directory and assign minimal rights. For more information on how to perform this task, see the "Setting the Access Control Lists for Active Directory" section on page 19.
Directory Administrator Password	Enter the password for the Directory Administrator DN user.
Confirm Password	Enter the password again.
Cisco Directory Configuration DN	Enter the Cisco Directory Configuration Distinguished Name. This field specifies the DN where the Cisco-dependent schema is created for the Cisco Unified CallManager.
User Search Base	Enter the User Search Base. Cisco Unified CallManager searches for users under this base.
User Creation Base	Enter the User Creation Base. Any user that is created by using Cisco Unified CallManager Administration resides under this node in the directory. **Note** Make the user creation base the same as the User Search Base or a subtree under the User Search Base. If you do not, you cannot look up users that you create in Cisco Unified CallManager Administration.
User Search Attribute	Enter an attribute that you can use to search for a user in the enterprise directory. Make sure that the value for this attribute is unique for each user in the directory. Examples include **mail** or **uid**. **Note** The user enters the value for this attribute in the User Identification field when the user logs in to the Cisco Unified IP Phone User Options window.
Domain Name	Enter the Microsoft Active Directory domain name.

Step 20 If you are satisfied with the Active Directory configuration information, click **Next**.

Step 21 The Configure LDAP over SSL dialog box displays. If you want security implemented, check the Enable LDAP over SSL check box; otherwise, click the **Next** button and continue with Step 9.

Step 22 If you checked the Enable LDAP over SSL check box, enter the SSL port number (the default port number specifies 636).

Step 23 To continue the security configuration process, you must copy the certificate of CA that has issued the SSL certificate that is installed on the directory server to the publisher server. You need to enter this certificate filename needs in the text box next to the **Browse** button (or use the **Browse** button to find the copy of the file that is on the publisher server).

Note The first time that you configure security, copy the certificate to the publisher server and specify the path to that file in the text box that is on the Configure LDAP over SSL window. If this is an upgrade and SSL is already enabled, copy the certificate file and specify the path only if the certificate changed since the previous installation/upgrade.

If you click **Browse**, a new window opens that allows you to find the certificate file that needs to be selected.

Step 24 Click the **Next** button. The system begins to verify whether you entered the configuration information correctly.

Step 25 After completing the configuration information, click the **Next** button. The verification process begins to check whether the previous information exists in the directory. If the information exists, a confirmation window displays and summarizes the information. Click the **Next** button.

Step 26 The plug-in attempts to read the schema update permission registry key on the destination Microsoft Active Directory server where the schema is installed.

Note Make sure that the registry entry HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\Schema Update Allowed is set on the Microsoft Active Directory server to **1**. This allows write access to the schema on that server.

Note The preceding registry entry value does not exist as a default on Microsoft AD 2003. To allow the plug-in to continue if it is the first time that the plug-in is being run for Microsoft AD 2003, you will need to create the Schema Updated Allowed registry entry value. Perform the steps in the "Creating the Schema Update Allowed Registry for AD 2003" section on page 19.

Step 27 The plug-in completes the configuration process and displays a dialog box. Click the **Finish** button and reboot the server immediately.

At the end of the installation on the publisher server, the plug-in reminds you to set the password for Cisco Unified CallManager system users before running the plug-in on Cisco Unified CallManager subscriber servers.

Caution Before you install the Cisco Customer Directory Configuration Plugin on the subscriber servers, you must perform the procedure that is described in "Enabling Cisco IP Services After Directory Integration on the Publisher Database Server (Required)" section on page 23. If you attempt to install the plug-in on

the subscriber servers before you perform the service integration procedure, the installation displays a message, and the Cisco Extended Functions, Cisco Unified CallManager Assistant (Cisco IPMA), and Cisco Unified CallManager Extension Mobility services do not function.

Creating the Schema Update Allowed Registry for AD 2003

If you are running the plug-in for the first time for Microsoft AD 2003, perform the following procedure to create the Schema Update Allowed registry:

Step 1 On the Microsoft AD 2003 Schema Master, choose **Start > Run**.

Step 2 Enter **regedit** and click **OK**.

Step 3 Expand the registry tree HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > NTDS > Parameters.

Step 4 Create Schema Update Allowed registry value under the Parameters heading as shown in the following list:

Name: Schema Update Allowed

Type: REG_DWORD

Data: 1

Setting the Access Control Lists for Active Directory

You do not have to use the Administrator User ID to enable the Cisco Unified CallManager to work with Active Directory. If you want to use a different account than the administrator account, you can create a user who corresponds to the Cisco Directory Administrator in the Active Directory as described in the following sections. You can name this user "dcd admin" and enter this user when prompted for the Directory Administrator DN in Step 19 of the "Integrating Microsoft Active Directory with Cisco Unified CallManager" section on page 12.

The dcd admin user receives only read permission to the "Users" object; therefore, you cannot create the dcd admin user from Cisco Unified CallManager Administration. You must create the dcd admin user with other methods, such as Active Directory Users and Computers, which the following sections describe. After you create the user, set the access control lists for this user.

The dcd admin user needs the following permissions in the Active Directory:

- The Access Control Lists set on Active Directory, so the Cisco Directory Administrator (dcd admin) has read/modify/write privileges on the ciscoatUserProfile, ciscoatUserProfilestring, and ciscoatGUID attributes in all user objects.
- Read permissions for all the attributes under all the User objects.
- Full control on the entire Cisco Directory Configuration DN. You need full control on this object and all objects under this object.

In the previous access lists, the dcd admin user received only the read rights to the Users Object in the Active Directory, which means that you cannot create new users through Cisco Unified CallManager Administration. As a common scenario in large enterprises, the corporate Active Directory team creates the new users, and other applications have read-only permissions to the user attributes.

To create the dcd admin and assign permissions, perform the following procedures after extending the Active Directory Schema:

- Creating a DCD Admin User, page 20
- Assigning Rights for ciscoatUserProfile, ciscoatuserProfileString, and ciscoatGUID, page 21
- Assigning Rights for CiscoOU, page 22

Creating a DCD Admin User

This section describes how to add a user in Active Directory that is equivalent to the DC Directory Administrator.

Step 1 On the Domain Controller, choose **Launch Start > Programs > Administrative Tools > Active Directory User and Computers**.

Step 2 Choose the top-level user container.

Step 3 Create a user in Active Directory that is equivalent to the DC Directory Administrator. For example, create a user named "dcd admin."

Step 4 Right-click the Users Container and choose **New > User**.

The New Object User window displays.

Step 5 In the First Name field, enter the first name of the administrative user, such as *dcd*.

Step 6 In the Last Name field, enter the last name of the administrative user, such as *admin*.

Step 7 In the User Logon Name field, enter the logon name of the administrative user, such as *dcdadmin*.

Step 8 Click **Next**.

Step 9 In the Password field, enter the password.

Step 10 In the Confirm Password field, enter the password again.

Step 11 Check the **Password Never Expires** check box.

Step 12 Click **Next**.

Step 13 Click **Finish**.

Active Directory creates the user. The Display Name matches the user name that you entered. For example, if you entered *dcd* in the First Name field and *admin* in the Last Name field, the display name displays as *dcd admin* (with a space).

In Step 19 of the "Integrating Microsoft Active Directory with Cisco Unified CallManager" section on page 12, enter the display name of this user in the Directory Administrator DN field. In this case, enter *dcd admin* (with a space).

Related Topics

- Assigning Rights for ciscoatUserProfile, ciscoatuserProfileString, and ciscoatGUID, page 21
- Assigning Rights for CiscoOU, page 22

Assigning Rights for ciscoatUserProfile, ciscoatuserProfileString, and ciscoatGUID

Use the following procedure to assign rights to the user that you created in the "Creating a DCD Admin User" section on page 20.

Step 1 On the Domain Controller, choose **Launch Start > Programs > Administrative Tools > Active Directory User and Computers**.

Step 2 Choose the top-level user container.

Step 3 Right-click and choose **Delegate Control**.

The Delegate Control Wizard Welcome window displays.

Step 4 Click **Next**.

The Selected Users or Groups window displays.

Step 5 Click **Add**.

Step 6 Choose the user to whom you want to assign the rights, such as dcd admin and click **Add**.

Step 7 Click **OK**.

The chosen user displays in the Selected Users and Groups list box.

Step 8 Click **Next**.

Step 9 In the Active Directory Object Type window, choose the **Only the following objects in this folder** radio button.

Step 10 Check the **User objects** check box and click **Next**.

Step 11 In the Permissions window, check the **General** and **Property-specific** check boxes.

Step 12 Check the **Read** check box.

The Wizard automatically checks all the read permissions as well as the Write ciscoatUserProfile, ciscoatUserProfileString, and ciscoatGUID permissions.

Step 13 Click **Next**.

A summary window displays.

Step 14 Click **Finish**.

Related Topics

- Creating a DCD Admin User, page 20
- Assigning Rights for CiscoOU, page 22

Assigning Rights for CiscoOU

This CiscoOU contains all the Cisco-specific attributes. Use the following procedure to give full permissions for the CiscoOU to the user that you created in the "Creating a DCD Admin User" section on page 20.

Step 1 On the Domain Controller, choose **Launch Start > Programs > Administrative Tools > Active Directory User and Computers**.

Step 2 Right-click the CiscoOU (for example, CiscoCM332) and choose **Delegate Control**.

Step 3 Click **Next**.

The Selected Users or Groups window displays.

Step 4 Click **Add**.

Step 5 Choose the user to whom you want to assign the rights; for example, *dcd admin*.

Step 6 Click **Add**.

Step 7 Click **OK**.

Step 8 The chosen user displays in the Selected Users and Groups list box.

Step 9 In the Tasks to Delegate window, choose the **Create a custom task to delegate** radio button and click **Next**.

Step 10 In the Active Directory Object Type window, choose the **This folder, existing objects in this folder, and creation of new objects in this folder** radio button and click **Next**.

Step 11 Check the **Full Control** check box and click **Next**.

Step 12 The summary of rights displays.

Step 13 Click **Finish**.

Related Topics

- Creating a DCD Admin User, page 20
- Assigning Rights for ciscoatUserProfile, ciscoatuserProfileString, and ciscoatGUID, page 21

Setting Access Control Lists for Netscape Directory

If any user that is not created by using the Cisco Unified CallManager Administration Add A new User window needs to be used as a Cisco Unified CallManager user, then Cisco Directory administrator (user "dcdadmin") should have write privileges over the attribute "objectclass." This privilege applies in addition to the other requirements that are stated for Active Directory.

Refer to the Netscape/iPlanet/SunOne directory administrator documentation for more information on how to set the access control.

Enabling Cisco IP Services After Directory Integration on the Publisher Database Server (Required)

Cisco Extended Functions, Cisco Tomcat, and Cisco Unified CallManager Extension Mobility services use a special user, **cn=CCMSysUser and mail=CCMSysUser (Netscape)** or **SAMAccountName=CCMSysUser (AD)**, to authenticate with Cisco Unified CallManager. You cannot view these users from Cisco Unified CallManager Administration. If you specify a User Search Attribute other than the default when you are configuring the plug-in, make sure that you set the value for the User Search Attribute for the CCMSysUser user to CCMSysUser. For example, if you specify **uid** as your User Search Attribute, edit the CCMSysUser user entry in your directory by setting uid to **CCMSysUser**.

In addition, when you integrate the Cisco Unified CallManager with Microsoft Active Directory, you must perform the following procedure to enable the Cisco Extended Functions, Cisco Tomcat, and Cisco CallManager Extension Mobility services.

Note Use this procedure for setting the password for special Cisco Unified CallManager system users rather than the procedure that previous versions of this document provided.

Step 1 While browsing into the publisher database server, choose **Start > Run** and enter **cmd** to open a command prompt. Click **OK**.

Step 2 Enter the command, **CCMPWDChanger**.

The Cisco Unified CallManager Password Changer window opens.

Step 3 In the Administrator Password field, enter the password of the user that was created to enable Cisco Unified CallManager to access the directory.

Step 4 Click **Next**.

The Cisco Unified CallManager Password Changer window displays. The User ID drop-down list box provides the following options: Directory Manager, CCMAdministrator, CCMSysUser, and IPMASysUser.

Step 5 You must change the passwords for the CCMAdministrator, CCMSysUser, and IPMASysUser accounts. From the User ID drop-down list box, choose **CCMAdministrator**, **CCMSysUser**, or **IPMASysUser**.

Step 6 In the New Password field, enter the new password.

Step 7 In the Confirm New Password field, enter the password again.

Step 8 Click **OK**.

A confirmation message displays.

Step 9 Click **OK**.

Step 10 For the CCMAdministrator, CCMSysUser, and the IPMASysUser, perform Step 5 through Step 9.

Step 11 Click **Exit**.

Step 12 Restart the Cisco Extended Functions, Cisco IP Manager Assistant, and Cisco CallManager Extension Mobility services on the server on which you installed the plug-in, so the password change takes effect. To restart a service, choose **Start > Programs > Administrative Tools > Services**. Choose a service in the list, right-click the service, and choose **Restart**.

Note Whenever you add a new Cisco Unified CallManager server to the cluster, repeat this procedure.

Importing Data from the LDIF Files to the Enterprise Directory

The LDAP Data Interchange Format stores LDAP data in flat files, which you use to configure your enterprise directory, so Cisco Unified CallManager can use it.

Tip If you run the plug-in in the Custom mode and choose only the Generate Configuration LDIF Files option, the plug-in does not perform any operations on the directory server, nor does the enterprise directory integrate with Cisco Unified CallManager. This option, instead, generates a set of LDIF files that you can use to configure your enterprise directory. After you configure the enterprise directory by using the LDIF files, you integrate your enterprise directory with Cisco Unified CallManager by running the plug-in on every server in the cluster, as described in Table 1, the installation section, and the integration sections. If you choose all the options in the Custom mode, you do not need to run the plug-in again after you import the LDIF file data to the directory.

To use the LDIF files that the plug-in generates, you must run a LDIF tool to process the files and import the data to the directory. If you want to do so, run the Cisco-provided LDIF tool, ldapmodify.exe; for information on how to use this tool, see the "Running ldapmodify.exe to Import LDIF File Data" section on page 25.

You create the configuration LDIF files and run the LDIF tool only once per cluster; that is, you do not need to run the plug-in on every server in the cluster to generate the configuration LDIF files. You run the LDIF tool only one time because the publisher database server and the subscriber servers integrate with the same directory. Cisco recommends that you generate the configuration LDIF files on the publisher database server and use ldapmodify.exe to configure the enterprise directory.

Note If you choose to use a third-party LDIF tool instead of the Cisco-provided LDIF tool, be aware that Cisco does not support third-party LDIF tools. If you need technical assistance with the third-party LDIF tool, contact the vendor directly.

When you run the LDIF tool, you must use the LDIF files in the following order:

Netscape Directory Server

1. C:\dcdsrvr\run\dcx500\config\ContainersAndSysProfiles.ldif—Creates the default containers and system profile
2. C:\dcdsrvr\run\dcx500\config\SpecialUserProfiles.ldif—Creates the profiles for Cisco-specific special users
3. C:\dcdsrvr\run\dcx500\config\SpecialUsers.ldif—Creates the Cisco-specific special users

Active Directory

1. C:\dcdsrvr\run\dcx500\config\AD\at_schema.ldif— Adds the attributes for schema updates
2. C:\dcdsrvr\run\dcx500\config\AD\oc_schema.ldif—Adds the object classes for schema updates
3. C:\dcdsrvr\run\dcx500\config\ContainersAndSysProfiles.ldif—Creates the default containers and system profile
4. C:\dcdsrvr\run\dcx500\config\SpecialUserProfiles.ldif—Creates the profiles for Cisco-specific special users
5. C:\dcdsrvr\run\dcx500\config\SpecialUsers_AD.ldif—Creates the Cisco-specific special users

Caution Failing to run the files in the order that is specified may cause problems with your enterprise directory.

Running ldapmodify.exe to Import LDIF File Data

If you choose not to use a third-party LDIF tool, you must run the Cisco-provided LDIF tool, ldapmodify.exe, that exists on any Cisco Unified CallManager server in the cluster. To run the ldapmodify.exe, perform the following procedure:

Procedure

Step 1 On the publisher database server, choose **Start > Run**.

Step 2 Enter **cmd**; click **OK**.

A Command Line Interface displays.

Step 3 Enter **C:** and press **Enter**.

Step 4 Enter **cd C:\dcdsrvr\bin\ldapsdk-508** and press **Enter**.

Step 5 By using Table 7 as a reference to define the variables, enter the command **ldapmodify.exe -h <server name> -p <port number> -D <admin DN> -w <admin Passwd> -c -a -f <i\p LDIF file> -e <Reject file>**

Table 7 Commands for ldapmodify.exe CLI

Command	Description
<server name>	Hostname or IP address of directory server
<port name>	Port number that is configured for the directory server
<admin DN>	Administrator DN (Distinguished Name) for the directory server **Note** Ensure that this name has permission to modify schema and to add entries under cisco base and user base.
<admin Passwd>	Administrator password
<i\p LDIF file>	Full path of the LDIF file from which data will import to the directory
<Reject file>	Full path of the LDIF file where you want to move rejected entries

Step 6 Close the CLI.

Restoring Applications After Directory Integration (Required If Application Is Installed)

After you run the Cisco Customer Directory Configuration Plugin, you need to restore any application that previously accessed the DC-Directory; for example, applications such as, but not limited to, IP IVR, Cisco Emergency Responder, Cisco SoftPhone, and Cisco Unified CallManager Attendant Console. If you are working with a new Cisco Unified CallManager installation and have not deployed any applications, you can skip this section.

Note Before performing any directory migrations, contact your Applications Administrator for more information. Applications include Cisco-provided applications or any third-party application that was developed for Cisco Unified CallManager.

Cisco Unified CallManager Attendant Console

You must reconfigure the "ac" user in Cisco Unified CallManager Administration and associate the attendant phones and the pilot points with the user. If you do not configure this user, the attendant console cannot interact with CTIManager. For more information, refer to the *Cisco Unified CallManager Administration Guide*.

Cisco Emergency Responder

With CER 1.1(1), you could use only DC-Directory. With CER 1.1(2), CER 1.1(3), and CER 1.1(4), you can use either DC-Directory or Active Directory. After integration with Active Directory takes place, you must reconfigure CER. For more detailed information on simplifying the reconfiguration and on Active Directory limitations, refer to the *Release Notes for Cisco Emergency Responder* at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_release_notes_list.html

If the directory is changed in CER 1.2(x), run the following program:

C:\Program Files\Cisco Systems\CiscoER\binAdminUtils\CERAdminUtility.exe

For more detailed information on troubleshooting, refer to the *Troubleshooting Cisco Emergency Responder* at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps842/products_administration_guide_chapter09186a00801af4aa.html

To restore CER, you must also migrate the Java Telephony Application Programming Interface (JTAPI) users. CER registers itself with some route points and CTI ports in Cisco Unified CallManager for its functionality (911, 913XXXXXXXXXX, and so on.). You associate these route points with a user name in the directory. After directory migration, you need to add the user again and reassociate the user with the route points and ports. If you do not make these associations properly, CER fails to handle emergency calls.

Cisco Intelligent Contact Management/IPCC

Migrating to Active Directory results in Intelligent Contact Management losing its associations with CTI route points, and CTI ports and agents no longer having control of their phones.

Note Before performing any directory migrations, contact your Intelligent Contact Management/IPCC Administrator for more information.

Cisco Personal Assistant

Cisco Personal Assistant stores all configuration information in the Cisco Unified CallManager directory. When you integrate with a different directory (Netscape or AD), you must reinstall and reconfigure Cisco Personal Assistant.

Cisco SoftPhone

To restore Cisco SoftPhone, enter the UserID and Password that are configured in the TSP into the directory (Netscape or AD). For more information about Cisco SoftPhone and TSP settings, refer to the *Cisco IP Softphone Administrator Guide*.

Adding and Deleting Users by Using Cisco Unified CallManager Administration

You can always modify Cisco-specific attributes; however, by default, you cannot add or delete user entries from your enterprise directory by using Cisco Unified CallManager Administration unless you modify the UMDirectoryConfiguration.ini file by using UpdateDirFlags.exe, as described in the following procedure.

This functionality, which is provided for your convenience, does not replace your existing user/directory management tools. Be aware that this functionality is limited; Cisco expects that you typically will add or delete users by using other available tools.

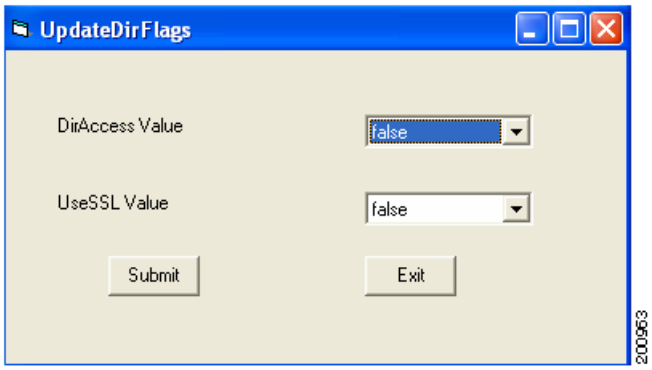
Note You cannot set up or update user passwords from Cisco Unified CallManager Administration when it is integrated with Microsoft Active Directory.

Caution Do not make any changes to the UMDirectoryConfiguration.ini or DirectoryConfiguration.ini configuration file manually. Instead, use the UpdateDirFlags.exe tool as described in the following procedure.

Before you add or delete users through Cisco Unified CallManager Administration, perform the following procedure:

Step 1 Browse to C:\dcdsrvr\bin and open the **UpdateDirFlags.exe** file. The UpdateDirFlags window displays as shown in Figure 1.

Figure 1 UpdateDirFlags Window



Step 2 From the DirAccess Value dropdown list, select **true**.

Step 3 Click **Submit**. An alert message displays as shown in Figure 2.

Figure 2 UpdateDirFlags Window Alert Message

Step 4 Click **OK**.

Step 5 To close the UpdateDirFlags window, click **Exit**.

Step 6 Restart the IIS Admin Service and its dependent services by choosing **Start>Programs> Administrative Tools>Services**.

Step 7 Right-click **IIS Admin Service** and choose **Restart**.

Step 8 A dialog box prompts you to restart dependent services. These services may differ depending on your configuration. Click **Yes**.

Step 9 Restart the dependent services.

You may now add, update, or delete users within Cisco Unified CallManager Administration. Refer to the latest version of the *Cisco Unified CallManager Administration Guide* for information on how to perform these tasks.

Caution When you are using Microsoft Active Directory and entering the user name and password in Cisco Unified CallManager Administration, make sure that you use only alphanumeric characters. Do not use the following special characters: / \ [ ] : ; | = , + * ? < >. Additionally, Cisco recommends that you do not use spaces.

Troubleshooting

The following section provides troubleshooting procedures for applications that use an enterprise directory.

Cisco Unified CallManager Assistant Console Cannot Access the Enterprise Directory

Cisco Unified CallManager provides a default directory that the assistant accesses from the Assistant Console. If the assistant needs access to a corporate directory (accessing Cisco Unified CallManager interclusters), you must update the LDAPConfig.ini file and store it on the primary and backup Cisco Unified CallManager Assistant servers. For more detailed information, refer to the *Cisco Unified CallManager Features and Services Guide*.

Personal Fast Dials and Personal Address Book Disappear

The Personal Address Book and Personal Fast Dials services use the samAccountName to build a directory structure to store information, as shown in Example 1. If you change the sAMAccountName on the enterprise directory server, you must rename the organization unit, *samAccountName*_info, with the new samAccountName.

Example 1 Personal Address Book and Personal Fast Dials Directory Structure

```
CCN
    user_info
        samAccountName_info
            FastDialEntries
            PersonalAddressBook
```

Installation Error Messages

Table 8 lists installation-related messages and corrective actions.

Table 8 Installation-Related Messages

Message	Corrective Action
Please ensure that the registry entry "HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\NTDS\Parameters\Schema Update Allowed" has been set on the Active Directory Server to "1" to permit Write access to the schema on that server. For more information please refer to Active Directory -> How To -> Manage the Schema" section in Windows 2000 online help.	The message contains the corrective action.
Setup failed to connect. Please enter your Host Name, Port Number, Directory Administrator DN and Password again.	The message contains the corrective action.
Setup failed to connect. Please enter your Host Name and Port Number.	The message contains the corrective action.
Publisher's host name for this Subscriber can't be empty or NULL.	The message contains the corrective action.
Fail to authenticate to Publisher.	Make sure the username and password match.
Failed to read remote registry to get password for "Directory Manager" on Publisher. Setup will be aborted now.	Make sure that you set the Directory Manager password on the publisher database server.
Failed to read remote registry to get password for "CCMAdministrator" on Publisher. Please set password on Publisher now.	Make sure that you set the CCMAdministrator password on the publisher database server.
Failed to read remote registry to get password for "CCMSysUser" on Publisher. Please set password on Publisher now.	Make sure that you set the CCMSysUser password on the publisher database server.
Failed to read remote registry to get password for "IPMASysUser" on Publisher. Please set password on Publisher now.	Make sure that you set the IPMASysUser password on the publisher database server.

Obtaining the Log Files

On each server in the cluster, the plug-in installation generates the log file, PluginSetUp.trc, under C:\dcdsrvr\log. The time stamp for each plug-in installation exists in the file. Whenever you reinstall or upgrade the plug-in, this log file gets appended. The plug-in installation generates other logs for the directory schema updates and configuration. These files get overwritten each time that you install the plug-in.

Before you contact your technical support team about any issues that are associated with the plug-in, obtain and review the log file for the plug-in installation, PluginSetUp.trc, and other log files that are mentioned in the PluginSetup.trc file.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the

Advanced Search link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html