



CHAPTER 17

LDAP Directory Integration

Last revised on: October 30, 2008

Directories are specialized databases that are optimized for a high number of reads and searches, and occasional writes and updates. Directories typically store data that does not change often, such as employee information, user privileges on the corporate network, and so on.

Another aspect of directories is that they are extensible, which means that the type of information stored in them can be modified and extended. The term *directory schema* refers to the type of stored information and the rules it obeys.

The Lightweight Directory Access Protocol (LDAP) provides applications with a standard method for accessing and potentially modifying the information stored in the directory. This capability enables companies to centralize all user information in a single repository available to several applications, with a remarkable reduction in maintenance costs through the ease of adds, moves, and changes.

This chapter covers the main design principles for integrating a Cisco IP Communications system based on Cisco Unified Communications Manager (Unified CM) 5.x with a corporate LDAP directory. The main topics include:

- [What is Directory Integration?, page 17-2](#)

This section analyzes the various requirements for integration with a corporate LDAP directory in a typical enterprise IT organization.

- [Directory Access for IP Telephony Endpoints, page 17-4](#)

This section describes the technical solution to enable directory access for Cisco Unified Communications endpoints and provides design best-practices around it.

- [Directory Integration with Unified CM 5.x, page 17-6](#)

This section describes the technical solutions and provides design best-practices for directory integration with Cisco Unified CM 5.x, including the LDAP synchronization and LDAP authentication functions.

The considerations presented in this chapter apply to Cisco Unified CM 5.x as well as the following applications bundled with it: Cisco Extension Mobility, Cisco Unified Communications Manager Assistant, WebDialer, Bulk Administration Tool, and Real-Time Monitoring Tool.

For earlier releases of Unified CM, refer to the appropriate version of the *Cisco Unified Communications SRND*; and for all other Cisco voice applications, refer to the respective product documentation available at:

<http://www.cisco.com>

In particular, for Cisco IP Contact Center refer to the *Cisco Cisco Unified Contact Center Enterprise Edition SRND* and the *Cisco Cisco Unified Contact Center Express SRND*, both available at

<http://www.cisco.com/go/designzone>

For Cisco Unity, refer to the *Cisco Unity Design Guide* and to the following white papers: *Cisco Unity Data and the Directory*, *Active Directory Capacity Planning*, and *Cisco Unity Data Architecture and How Cisco Unity Works*, also available at

<http://www.cisco.com>

What's New in This Chapter

Table 17-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

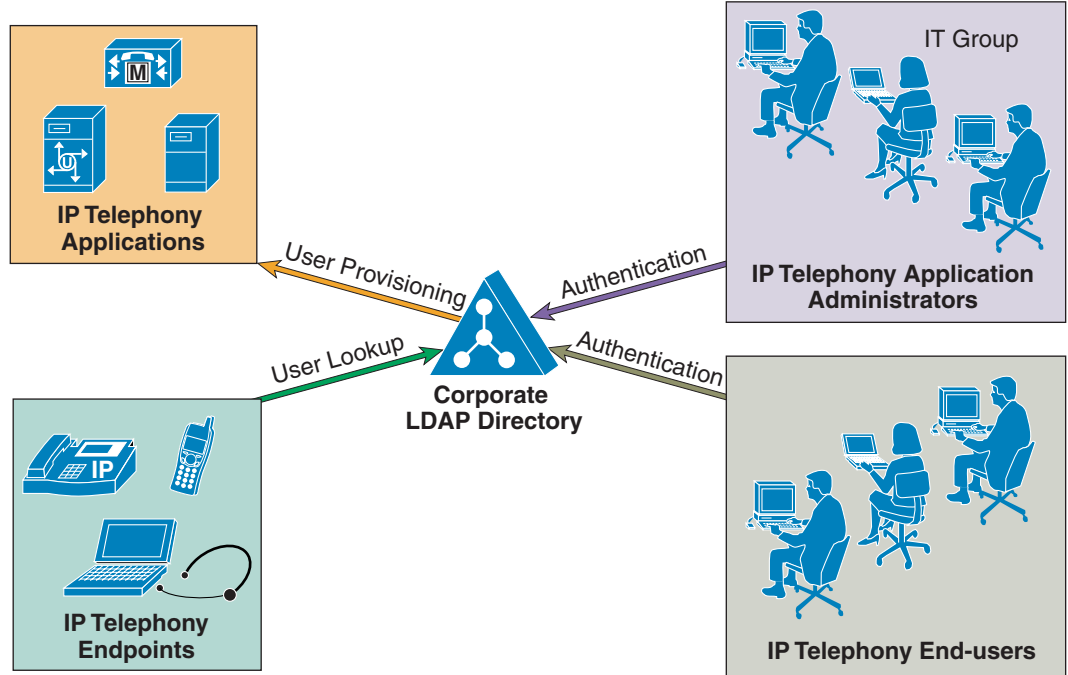
Table 17-1 ***New or Changed Information Since the Previous Release of This Document***

New or Revised Topic	Described in:
Directory synchronization	Using the LDAP Structure to Control Synchronization, page 17-25
The section on LDAP Query Filter was deleted from this chapter.	

What is Directory Integration?

Integration between voice applications and a corporate LDAP directory is a common task for many enterprise IT organizations. However, the exact scope of the integration varies from company to company, and it can translate to one or more specific and independent requirements, as shown in [Figure 17-1](#).

Figure 17-1 Various Requirements for Directory Integration



153279

For example, one common requirement is to enable user lookups (sometimes called the "white pages" service) from IP phones or other voice and/or video endpoints, so that users can dial a contact directly after looking up their number in the directory.

Another requirement is to provision users automatically from the corporate directory into the user database of voice and/or video applications. This method avoids having to add, remove, or modify core user information manually each time a change occurs in the corporate directory.

Often authentication of end-users and administrators of the voice and/or video applications using the corporate directory credentials is also required. This method enables the IT department to deliver single log-on functionality and reduces the number of passwords that each user needs to maintain across different corporate applications.

Each of these requirements can be satisfied by a Cisco IP Communications system using different mechanisms according to the Unified CM version used, as summarized in [Table 17-2](#).

Table 17-2 Directory Requirements and Cisco Solutions

Requirement	Cisco Solution	Cisco Unified CM 4.x Feature	Cisco Unified CM 5.x Feature
User lookup for endpoints	Directory access	Cisco Unified IP Phone Services SDK	Cisco Unified IP Phone Services SDK
User provisioning	Directory integration	Cisco Customer Directory Configuration Plugin	LDAP Synchronization

Table 17-2 Directory Requirements and Cisco Solutions (continued)

Requirement	Cisco Solution	Cisco Unified CM 4.x Feature	Cisco Unified CM 5.x Feature
Authentication for IP Telephony end users	Directory integration	Cisco Customer Directory Configuration Plugin	LDAP Authentication
Authentication for IP Telephony application administrators	Directory integration	Cisco Customer Directory Configuration Plugin + Cisco Multilevel Administration	LDAP Authentication

As shown in [Table 17-2](#), within the context of a Cisco IP Communications system, the term *directory access* refers to mechanisms and solutions that satisfy the requirement of user lookups for IP Telephony endpoints, while the term *directory integration* refers to mechanisms and solutions that satisfy the requirements of user provisioning and authentication (for both end users and administrators).

The remainder of this chapter describes how to address these requirements in a Cisco IP Communications system based on Cisco Unified CM Release 5.x. For a detailed description of directory integration solutions with earlier releases of Unified CM, refer to the appropriate version of the *Cisco Unified Communications SRND*, available at

<http://www.cisco.com/go/designzone>

**Note**

Another interpretation of the term *directory integration* revolves around the ability to add application servers to a Microsoft Active Directory domain in order to centralize management and security policies. Cisco Unified CM 5.x is an appliance that runs on a customized embedded operating system, and it cannot currently be added to a Microsoft Active Directory domain. Server management for Unified CM is provided through the Cisco Real Time Monitoring Tool (RTMT). Strong security policies tailored to the application are already implemented within the embedded operating system, and a customized version of Cisco Security Agent can be installed on every server. It is also possible to manage security policies centrally with the CiscoWorks Management Center for Cisco Security Agents.

Directory Access for IP Telephony Endpoints

This section describes how to configure corporate directory access to any LDAP-compliant directory server to perform user lookups from Cisco Unified Communications endpoints (such as Cisco Unified IP Phones). The guidelines contained in this section apply regardless of whether Unified CM or other IP Telephony applications have been integrated with a corporate directory for user provisioning and authentication.

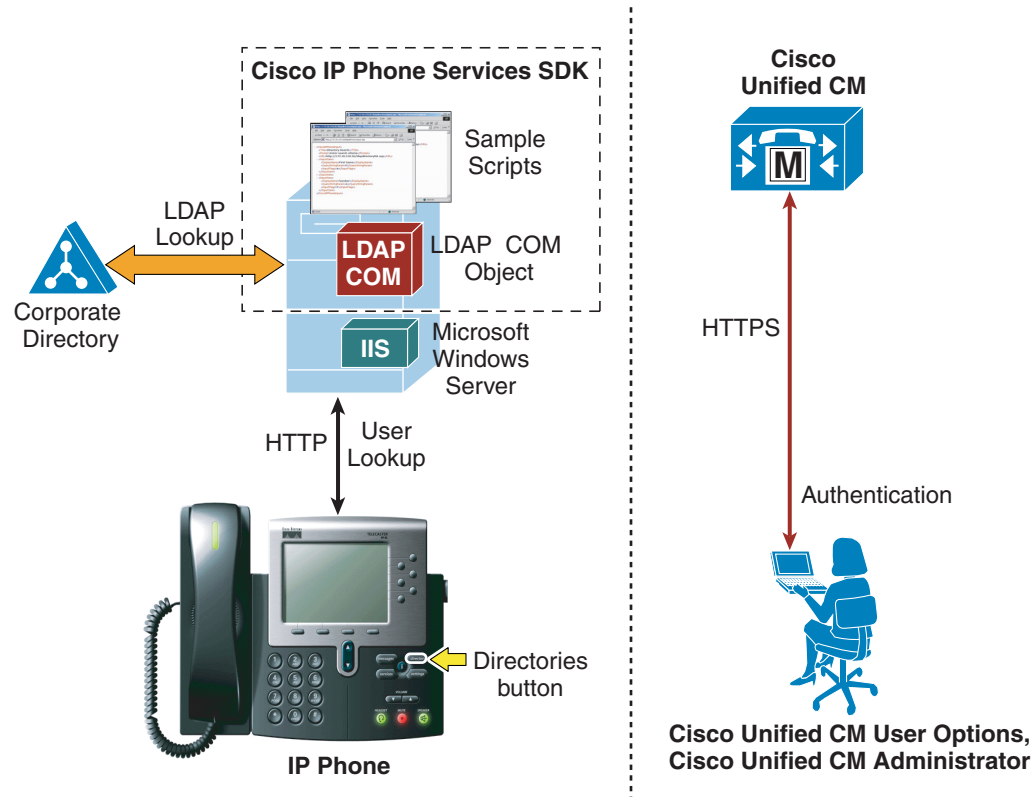
Cisco Unified IP Phones equipped with a display screen can search a user directory when a user presses the Directories button on the phone. The IP Phones use Hyper-Text Transfer Protocol (HTTP) to send requests to a web server. The responses from the web server must contain some specific Extensible Markup Language (XML) objects that the phone can interpret and display.

By default, Cisco Unified IP Phones are configured to perform user lookups against Unified CM's embedded database. However, it is possible to change this configuration so that the lookup is performed on a corporate LDAP directory. In this case, the phones send their HTTP requests to an external web

server that operates as a proxy and translates these requests into LDAP queries against the corporate directory. The LDAP responses are then encapsulated in the appropriate XML objects and sent back to the phones via HTTP.

Figure 17-2 illustrates this mechanism in a deployment where Unified CM has not been integrated with the corporate directory. Note that, in this scenario, Unified CM is not involved in the message exchange related to the user lookup.

Figure 17-2 Directory Access for Cisco Unified IP Phones Using the Cisco Unified IP Phone Services SDK



In the example shown in Figure 17-2, the web server proxy function is provided by the Cisco LDAP Search Component Object Model (COM) server, which is included in the Cisco Unified IP Phone Services Software Development Kit (SDK) version 3.3(4) or later. You can download the latest Cisco Unified IP Phone Services SDK from Cisco Developer Support Central at

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

The IP Phone Services SDK can be installed on a Microsoft Windows web server running IIS 4.0 or later, but it cannot be installed on a Unified CM server. The SDK includes some sample scripts to provide simple directory lookup functionality.

To set up a corporate directory lookup service using the IP Phone Services SDK, perform the following steps:

-
- Step 1** Modify one of the sample scripts to point to your corporate LDAP directory, or write your own script using the LDAP Search COM Programming Guide provided with the SDK.
 - Step 2** In Unified CM, configure the URL Directories parameter (under **System > Enterprise Parameters**) to point to the URL of the script on the external web server.
 - Step 3** Reset the phones to make the changes take effect.
-

**Note**

If you want to offer the service only to a subset of users, configure the URL Directories parameter directly within the Phone Configuration page instead of the Enterprise Parameters page.

In conclusion, the following design considerations apply to directory access with the Cisco Unified IP Phone Services SDK:

- User lookups are supported against any LDAP-compliant corporate directory.
- When querying Microsoft Active Directory, you can perform lookups against the Global Catalog by pointing the script to a Global Catalog server and specifying port 3268 in the script configuration. This method typically results in faster lookups.
- There is no impact on Unified CM for this functionality, and only minimal impact on the LDAP directory server.
- The sample scripts provided with the SDK allow only a minimal amount of customization (for example, you can prefix a digit string to all returned numbers). For a higher degree of manipulation, you will have to develop custom scripts, and a programming guide is included with the SDK to aid in writing the scripts.
- This functionality does not entail provisioning or authentication of Unified CM users with the corporate directory.

Directory Integration with Unified CM 5.x

This section describes the mechanisms and best practices for directory integration with Cisco Unified CM 5.x to allow for user provisioning and authentication with a corporate LDAP directory. This section covers the following topics:

- [Comparison with the Unified CM 4.x Approach, page 17-7](#)

The approach to directory integration has changed significantly between Unified CM releases 4.x and 5.x, and this section introduces the new approach by comparing it with the old one.

- [Unified CM 5.x Directory Architecture, page 17-8](#)

This section provides an overview of the user-related architecture in Unified CM 5.x.

- [LDAP Synchronization, page 17-11](#)

This section describes the functionality of LDAP synchronization and provides design guidelines for its deployment, with additional considerations for Microsoft Active Directory.

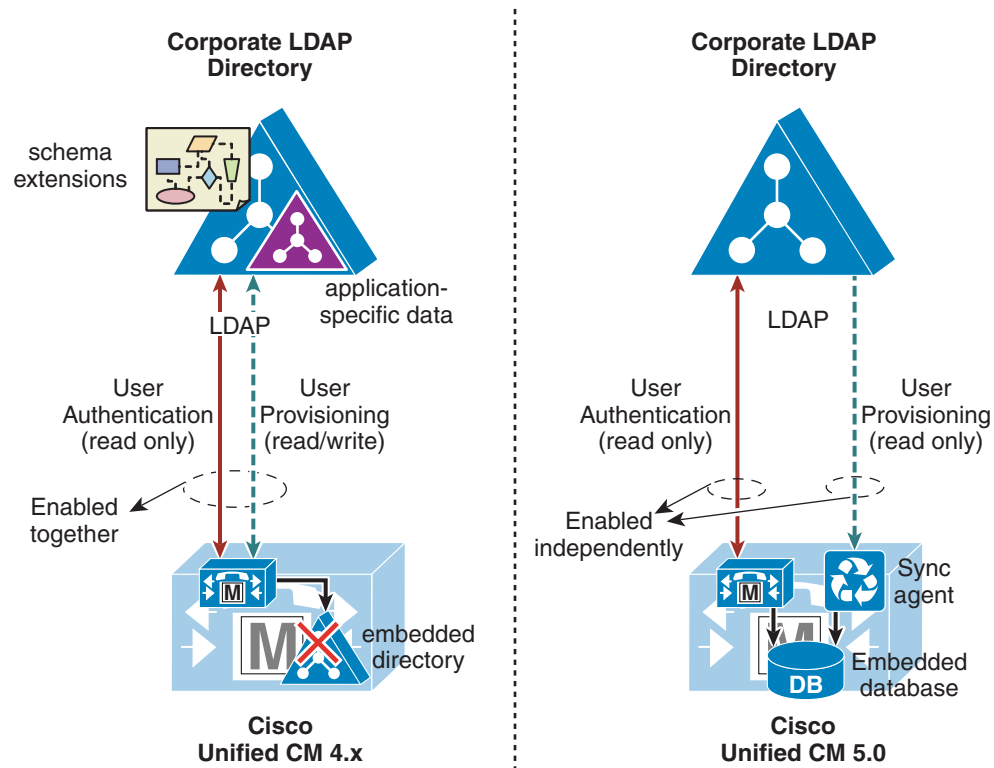
- [LDAP Authentication, page 17-19](#)

This section describes the functionality of LDAP authentication and provides design guidelines for its deployment, with additional considerations for Microsoft Active Directory.

Comparison with the Unified CM 4.x Approach

Figure 17-3 shows high-level functional diagrams of the directory integration approaches for user provisioning and authentication with Unified CM 4.x and 5.x.

Figure 17-3 Directory Integration Approaches in Unified CM 4.x and 5.x



Cisco Unified CM Release 4.x used an embedded LDAP directory to store user-related information. Directory integration was enabled by extending the corporate directory schema, shutting down the embedded directory, and using the corporate directory to store the application-specific data related to the users. Because the corporate directory was effectively used as the back-end storage repository for user information, this method satisfied the requirement for both user provisioning and user authentication. Any changes to user data in the corporate directory were immediately picked up by Unified CM because it accessed the same data store.

However, this approach had an impact on the corporate directory in terms of schema extensions and additional data, and it also introduced dependencies between the real-time functionality of the IP Communications system and the availability of the directory. When connectivity was lost or the directory became unavailable, Unified CM was unable to access all user-related configurations, which impacted applications such as Extension Mobility, Attendant Console, and IP Contact Center Express. In this approach, the user provisioning and user authentication functions had to be enabled at the same time

because they relied on the same integration process. In addition, using the corporate directory as the storage repository for application-specific data also imposed limitations on the day-to-day maintenance operations on the corporate directory itself.

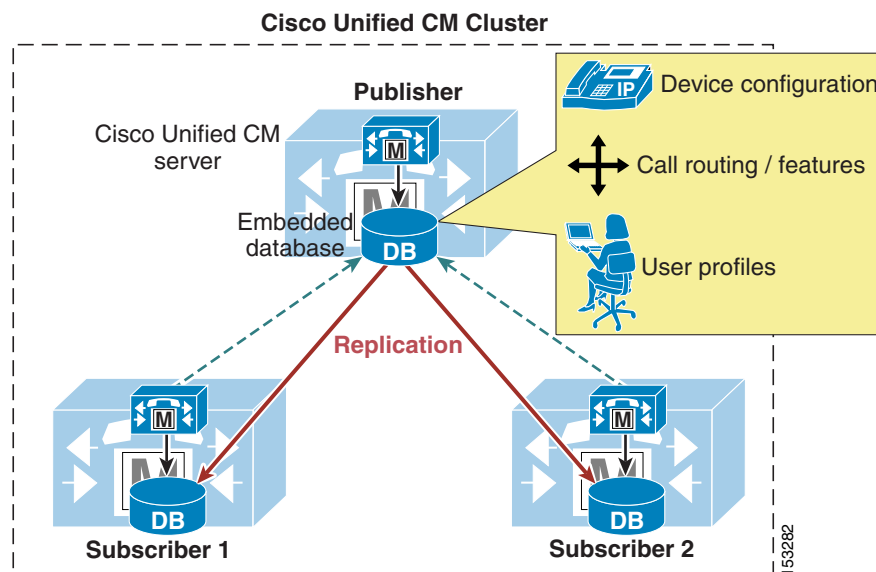
By contrast, the approach to directory integration adopted by Cisco Unified CM 5.x relies on two separate components to satisfy the user provisioning and user authentication requirements independently. User provisioning is performed with a one-way synchronization of user data from the corporate directory to the Unified CM embedded database. The synchronization uses standard LDAPv3 and can be triggered manually or scheduled periodically to ensure that changes are incorporated into the Cisco IP Communications system. This solution avoids the need to write anything to the corporate directory, and it does not require any schema extensions.

User authentication is enabled independently from user provisioning, and it provides authentication of end-user passwords against the corporate directory credentials. With this approach, the Cisco IP Communications system preserves all of its real-time functionality even when the corporate directory is unavailable or unreachable.

Unified CM 5.x Directory Architecture

Figure 17-4 shows the basic architecture of a Unified CM 5.x cluster. The embedded database stores all configuration information, including device-related data, call routing, and other features and user profiles. The database is present on all servers within a Unified CM cluster and is replicated automatically from the publisher server to all subscriber servers.

Figure 17-4 Cisco Unified CM 5.x Architecture



By default, all users are provisioned manually into the database via the Unified CM Administration interface. Cisco Unified CM 5.x introduces an important new concept by dividing the users in its database in two categories:

- End users — All users associated with a physical person and an interactive login. This category includes all IP Telephony users as well as Unified CM administrators when using the User Groups and Roles configuration (equivalent to the Cisco Multilevel Administration feature in prior Unified CM versions).
- Application users — All users associated with other Cisco IP Communications features or applications, such as Cisco Attendant Console, Cisco IP Contact Center Express, or Cisco Unified Communications Manager Assistant. These applications need to authenticate with Unified CM, but these internal "users" do not have an interactive login and serve purely for internal communications between applications.

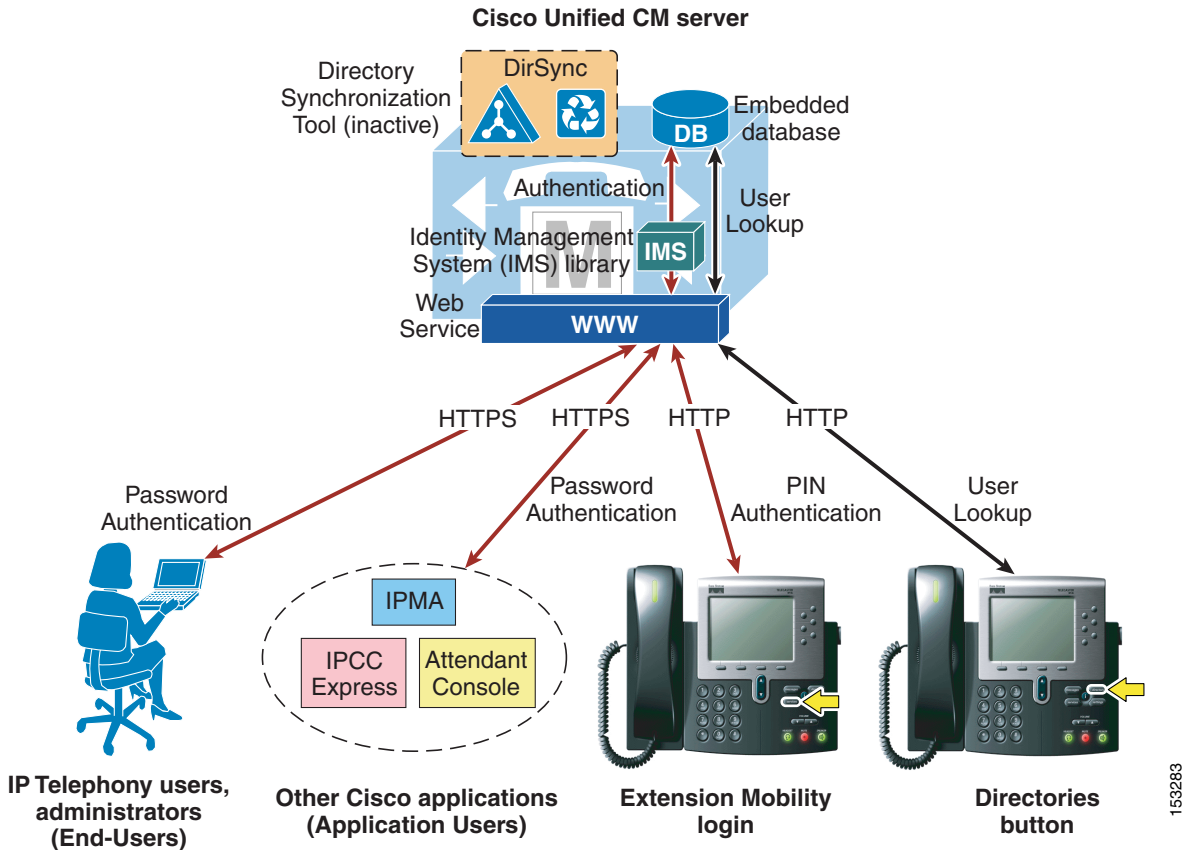
[Table 17-3](#) lists the application users created by default in the Unified CM database, together with the feature or application that uses them. Additional application users can be created manually when integrating other Cisco IP Communications applications (for example, the **ac** application user for Cisco Attendant Console, the **jtapi** application user for Cisco IP Contact Center Express, and so forth).

Table 17-3 Default Application Users for Unified CM 5.x

Application User	Used by:
CCMAdministrator	Unified CM Administration (default "super user")
CCMQRTSecureSysUser	Cisco Quality Reporting Tool
CCMQRTSysUser	
CCMSysUser	Cisco Extension Mobility
IPMASecureSysUser	Cisco Unified Communications Manager Assistant
IPMASysUser	
WDSecureSysUser	Cisco WebDialer
WDSysUser	

Based on these considerations, [Figure 17-5](#) illustrates the default behavior in Unified CM 5.x for user-related operations such as lookups, provisioning, and authentication.

Figure 17-5 Default Behavior for User-Related Operations for Unified CM 5.x



End users access the Unified CM User Options page via HTTPS and authenticate with a user name and password. If they have been configured as administrators by means of User Groups and Roles, they also access the Unified CM Administration pages with the same credentials.

Similarly, other Cisco features and applications authenticate to Unified CM via HTTPS with the user name and password associated with their respective application users.

The authentication challenges carried by the HTTPS messages are relayed by the web service on Unified CM to an internal library called Identity Management System (IMS). In its default configuration, the IMS library authenticates both end users and application users against the embedded database. In this way, both "physical" users of the IP Communications system and internal application accounts are authenticated using the credentials configured in Unified CM.

End users may also authenticate with their user name and a numeric password (or PIN) when logging into the Extension Mobility service from an IP phone. In this case, the authentication challenge is carried via HTTP to Unified CM but is still relayed by the web service to the IMS library, which authenticates the credentials against the embedded database.

In addition, user lookups performed by IP Telephony endpoints via the Directories button communicate with the web service on Unified CM via HTTP and access data on the embedded database.

The importance of the distinction between End Users and Application Users becomes apparent when integration with a corporate directory is required. As mentioned in the previous section, this integration is accomplished by means of the following two separate processes:

- LDAP synchronization

This process uses an internal tool called Cisco Directory Synchronization (DirSync) on Unified CM to synchronize a number of user attributes (either manually or periodically) from a corporate LDAP directory. When this feature is enabled, users are automatically provisioned from the corporate directory. This feature applies only to End Users, while Application Users are kept separate and are still provisioned via the Unified CM Administration interface. In summary, End Users are defined in the corporate directory and synchronized into the Unified CM database, while Application Users are stored only in the Unified CM database and do not need to be defined in the corporate directory.

- LDAP authentication

This process enables the IMS library to authenticate user credentials against a corporate LDAP directory. When this feature is enabled, End User passwords are authenticated against the corporate directory, while Application User passwords are still authenticated locally against the Unified CM database. Cisco Extension Mobility PINs are also still authenticated locally.

Maintaining and authenticating the Application Users internally to the Unified CM database provides resilience for all the applications and features that use these accounts to communicate with Unified CM, independently of the availability of the corporate LDAP directory.

Cisco Extension Mobility PINs are also kept within the Unified CM database because they are an integral part of a real-time application, which should not have dependencies on the responsiveness of the corporate directory.

The next two sections describe in more detail LDAP synchronization and LDAP authentication, and they provide design best-practices for both functions.

**Note**

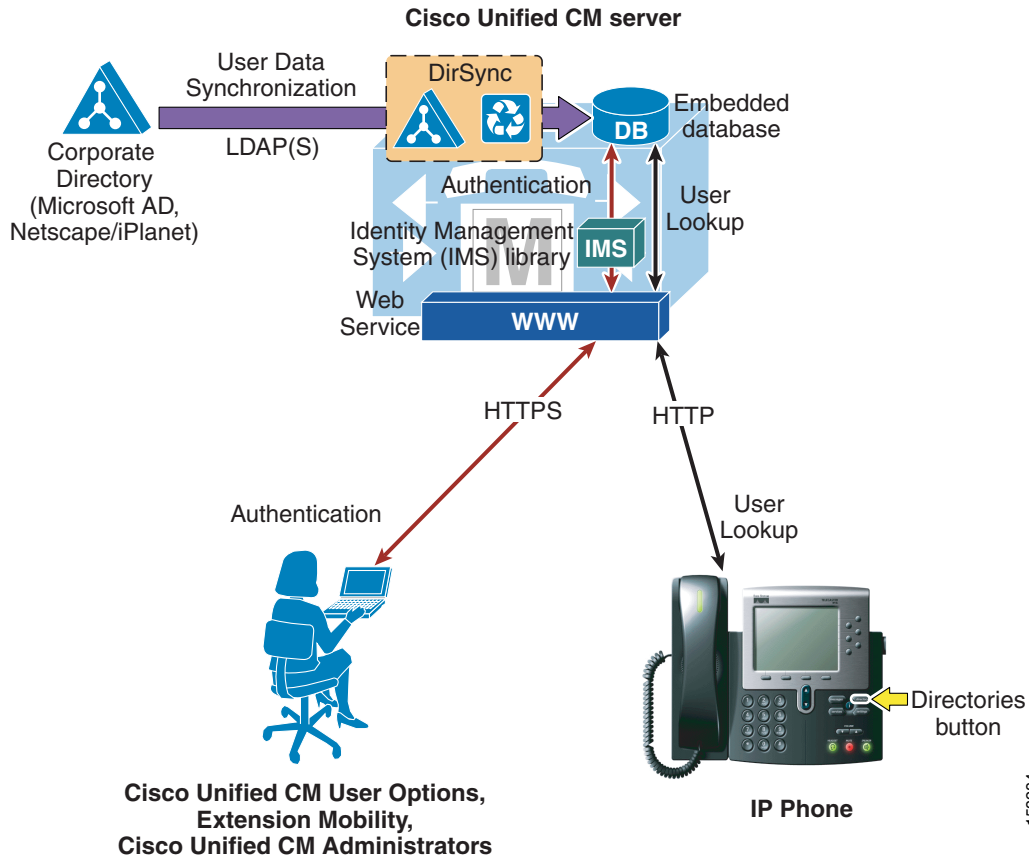
As illustrated in the section on [Directory Access for IP Telephony Endpoints](#), page 17-4, user lookups from endpoints can also be performed against a corporate directory by configuring the Cisco Unified IP Phone Services SDK on an external web server.

LDAP Synchronization

Synchronization of Unified CM with a corporate LDAP directory allows reuse of user data stored in the LDAP directory and allows the corporate LDAP directory to serve as the central repository for that information. Unified CM has an integrated database for storing user data and a web interface within Unified CM Administration for creating and managing user data in that database. When synchronization is enabled, that local database is still used, but the Unified CM facility to create user accounts becomes disabled. Management of user accounts is then accomplished through the interface of the LDAP directory. (See [Figure 17-6](#).)

The user account information is imported from the LDAP directory into the database located on the Unified CM publisher server. Information that is imported from the LDAP directory may not be changed by Unified CM. Additional user information specific to the Unified CM implementation is managed by Unified CM and stored only within its local database. For example, device-to-user associations, speed dials, and user PINs are data that are managed by Unified CM, and they do not exist in the corporate LDAP directory. The user data is then propagated from the Unified CM publisher server to the subscribers via the built-in database synchronization.

Figure 17-6 Enabling Synchronization of User Data



The following directories are supported by Unified CM for synchronization:

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

When LDAP synchronization is activated, only one of the above groups of LDAP products may be chosen for the cluster at any one time. Also, one attribute of the directory user is chosen to map into the Unified CM User ID field. Unified CM uses standard LDAPv3 for accessing the data.

The data that Unified CM imports are all from standard attributes. Table 17-4 lists the attributes that are used, and they differ between the two groups of LDAP implementations. The data of the directory attribute that is mapped to the Unified CM User ID must be unique within all entries for that cluster. The **sn** attribute must be populated with data, otherwise that record will not be imported from the corporate directory. If the primary attribute used during import of end user accounts matches any Application User in the Unified CM database, that user is not imported from the LDAP directory.

Table 17-4 lists the attributes that are imported from the LDAP directory into corresponding Unified CM user fields, and it describes the mapping between those fields. Some Unified CM user fields might be mapped from one of several LDAP attributes.

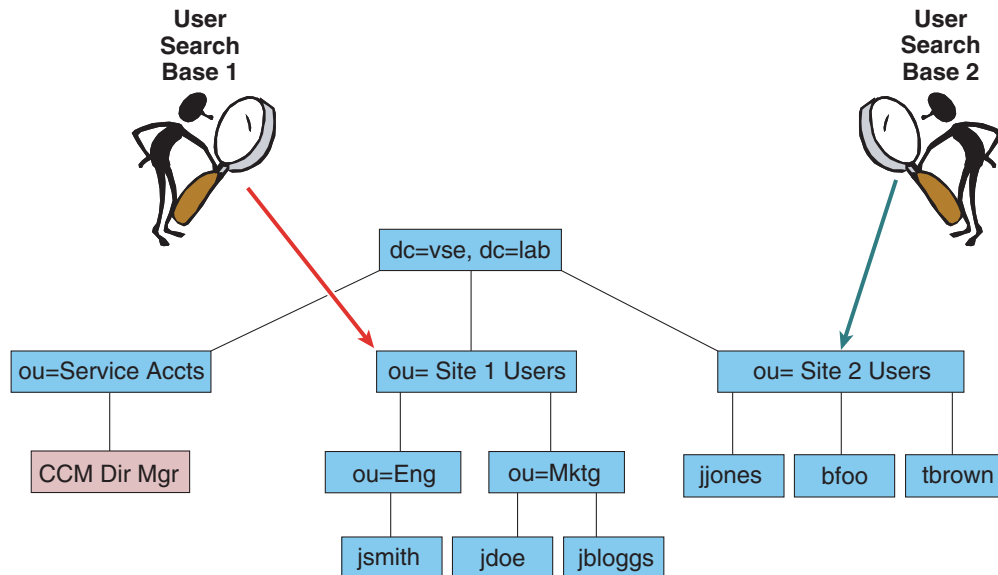
Table 17-4 Data Attributes Imported by Unified CM

Unified CM User Field	Microsoft Active Directory (AD) Attribute	Netscape, iPlanet, or Sun ONE Attribute
User ID	<i>One of:</i> sAMAccountName mail employeeNumber telephoneNumber UserPrincipalName	<i>One of:</i> uid mail employeeNumber telephonePhone
First Name	givenName	givenname
Middle Name	<i>One of:</i> middleName initials	initials
Last Name	sn	sn
Manager ID	manager	manager
Department	department	departmentnumber
Phone Number	<i>One of:</i> telephoneNumber ipPhone	telephonenumber
Mail ID	<i>One of:</i> mail sAMAccountName	<i>One of:</i> mail uid

The synchronization is performed by a process called Cisco DirSync, which is enabled through the Serviceability web page. When enabled, it allows one of five synchronization agreements to be configured in the system. An agreement specifies a search base that is a position in the LDAP tree where Unified CM will begin its search for user accounts. Unified CM can import only users that exist in the domain specified by the search base for a particular synchronization agreement.

In [Figure 17-7](#), two synchronization agreements are represented. One synchronization agreement specifies User Search Base 1 and imports users jsmith, jdoe and jblogs. The other synchronization agreement specifies User Search Base 2 and imports users jjones, bfoo, and tbrown. The CCMDirMgr account is not imported because it does not reside below the point specified by a user search base. When users are organized in a structure in the LDAP directory, you can use that structure to control which user groups are imported. In this example, a single synchronization agreement could have been used to specify the root of the domain, but that search base would also have imported the Service Accts. The search base does not have to specify the domain root; it may specify any point in the tree.

Figure 17-7 User Search Bases



153285

To import the data into the Unified CM database, the system performs a bind to the LDAP directory using the account specified in the configuration as the LDAP Manager Distinguished Name, and reading of the database is done with this account. The account must be available in the LDAP directory for Unified CM to log in, and Cisco recommends that you create a specific account with permissions to allow it to read all user objects within the sub-tree that was specified by the user search base. The sync agreement specifies the full Distinguished Name of that account so that the account may reside anywhere within that domain. In the example in [Figure 17-7](#), CCMDirMgr is the account used for the synchronization.

It is possible to control the import of accounts through use of permissions of the LDAP Manager Distinguished Name account. In this example, if that account is restricted to have read access to ou=Eng but not to ou=Mktg, then only the accounts located under Eng will be imported.

Synchronization agreements have the ability to specify multiple directory servers to provide redundancy. You can specify an ordered list of up to three directory servers in the configuration that will be used when attempting to synchronize. The servers are tried in order until the list is exhausted. If none of the directory servers responds, then the synchronization fails, but it will be attempted again according to the configured synchronization schedule.

Synchronization Mechanism

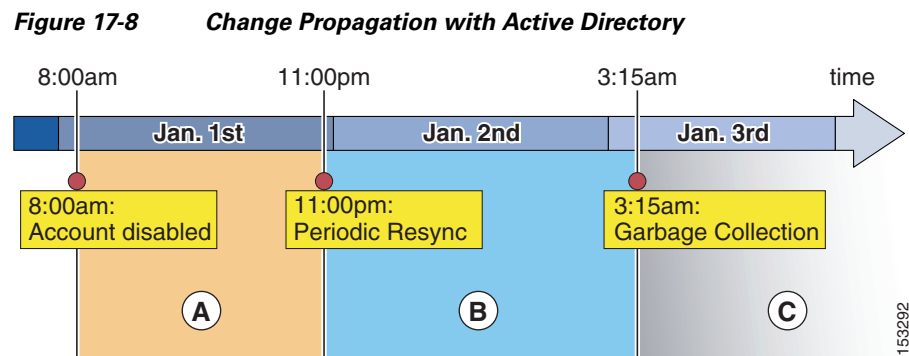
The synchronization agreement specifies a time for synchronizing to begin and a period for re-synchronizing that can be specified in hours, days, weeks, or months (with a minimum value of 6 hours). A synchronization agreement can also be set up to run only once at a specific time.

When synchronization is enabled for the first time on a Unified CM publisher server, user accounts that exist in the corporate directory are imported into the Unified CM database. Then either existing Unified CM end-user accounts are activated and data is updated, or a new end-user account is created according to the following process:

1. If end-user accounts already exist in the Unified CM database and a synchronization agreement is configured, all pre-existing accounts are marked inactive in Unified CM. The configuration of the synchronization agreement specifies a mapping of an LDAP database attribute to the Unified CM UserID. During the synchronization, accounts from the LDAP database that match an existing Unified CM account cause that Unified CM account to be marked active again.
2. After the synchronization is completed, any accounts that were not set to active are permanently deleted from Unified CM when the garbage collection process runs. Garbage collection is a process that runs automatically at the fixed time of 3:15 AM, and it is not configurable. The deletion of Unified CM accounts that do not match LDAP directory accounts is necessary because Unified CM cannot manage accounts while synchronization is configured.
3. Subsequently when changes are made in the corporate directory, the synchronization from Microsoft Active Directory occurs as a full re-synchronization at the next scheduled synchronization period. On the other hand, the Netscape, iPlanet, and Sun ONE products perform an incremental synchronization triggered by a change in the directory. The following sections present examples of each of these two scenarios.

Account Synchronization with Active Directory

Figure 17-8 shows an example timeline of events for a Unified CM deployment where LDAP Synchronization and LDAP Authentication have both been enabled. The re-synchronization is set for 11:00 PM daily.



After the initial synchronization, the creation, deletion, or disablement of an account will propagate to Unified CM according to the timeline shown in Figure 17-8 and as described in the following steps:

1. At 8:00 AM on January 1, an account is disabled or deleted in AD. From this time and during the whole period A, password authentication (for example, Unified CM User Options page) will fail for this user because Unified CM redirects authentication to AD. However, PIN authentication (for example, Extension Mobility login) will still succeed because the PIN is stored in the Unified CM database.
2. The periodic re-synchronization is scheduled for 11:00 PM on January 1. During that process, Unified CM will verify all accounts. Any accounts that have been disabled or deleted from AD will at that time be tagged in the Unified CM database as inactive. After 11:00 PM on January 1, when the account is marked inactive, both the PIN and password authentication by Unified CM will fail.

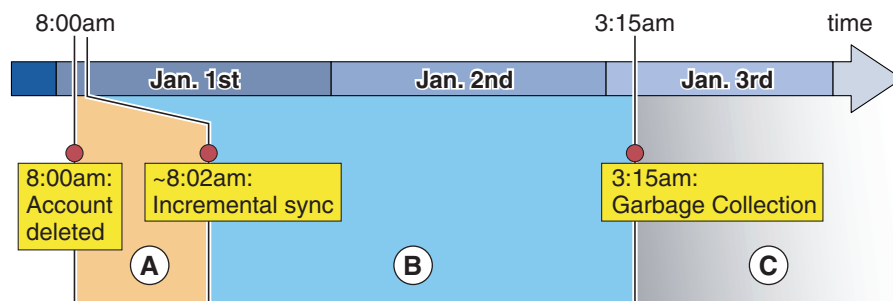
- Garbage collection of accounts occurs daily at the fixed time of 3:15 AM. This process permanently deletes user information from the Unified CM database for any record that has been marked inactive for over 24 hours. In this example, the garbage collection that runs at 3:15 AM on January 2 does not delete the account because it has not been inactive for 24 hours yet, so the account is deleted at 3:15 AM on January 3. At that point, the user data is permanently deleted from Unified CM.

If an account has been created in AD at the beginning of period A, it will be imported to Unified CM at the periodic re-synchronization that occurs at the beginning of period B and will immediately be active on Unified CM.

Account Synchronization with Netscape, iPlanet, or Sun ONE

The Netscape, iPlanet, and Sun ONE products support incremental synchronization agreements and use a different synchronization timeline than Active Directory. [Figure 17-9](#) shows an example of this synchronization timeline for a Unified CM deployment with LDAP Synchronization and LDAP Authentication both enabled.

Figure 17-9 Change Propagation with Netscape, iPlanet, and Sun ONE



The example in [Figure 17-9](#) involves the following steps:

- An account is deleted from the corporate directory at 8:00 AM on January 1, which causes an incremental update to be sent from the LDAP server to Unified CM. Unified CM sets its corresponding copy of the data to inactive. Because LDAP authentication is configured, the user will be unable to log in via password as soon as the LDAP server has deleted the record. Also, the PIN may not be used for login at the moment the Unified CM record is marked inactive.
- During period B, the user's record is still present in Unified CM, albeit inactive.
- When the garbage collection runs at 3:15 AM on January 2, the record has not yet been inactive for 24 hours. The data remains in the Unified CM database until the beginning of period C on January 3, when the garbage collection process runs again at 3:15 AM and determines that the record has been inactive for 24 hours or more. The record is then permanently deleted from the database.

Accounts that are newly created in the directory are synchronized to Unified CM via incremental updates as well, and they may be used as soon as the incremental update is received.

Security Considerations

During the import of accounts, no passwords or PINs are copied from the LDAP directory to the Unified CM database. If LDAP authentication is not enabled on Unified CM, the password and PIN for the end user are managed using Unified CM Administration. By default, the password is set to **ciscocisco** and the PIN is set to **12345** when the account is created. These settings can be changed by the user via

the user web pages or by the administrator via the administrator web pages. The password and PIN are stored in an encrypted format in the Unified CM database. If you want to use the directory password to authenticate an end user, see the section on [LDAP Authentication, page 17-19](#).

The connection between the Unified CM publisher server and the directory server can be secured by enabling Secure LDAP (SLDAP) on Unified CM and the LDAP server. Secure LDAP enables LDAP to be sent over a Secure Socket Layer (SSL) connection and can be enabled by uploading the SSL certificate from within the Unified CM Platform Administration. For detailed procedure steps, refer to the Unified CM product documentation available at <http://www.cisco.com>.

Best Practices for LDAP Synchronization

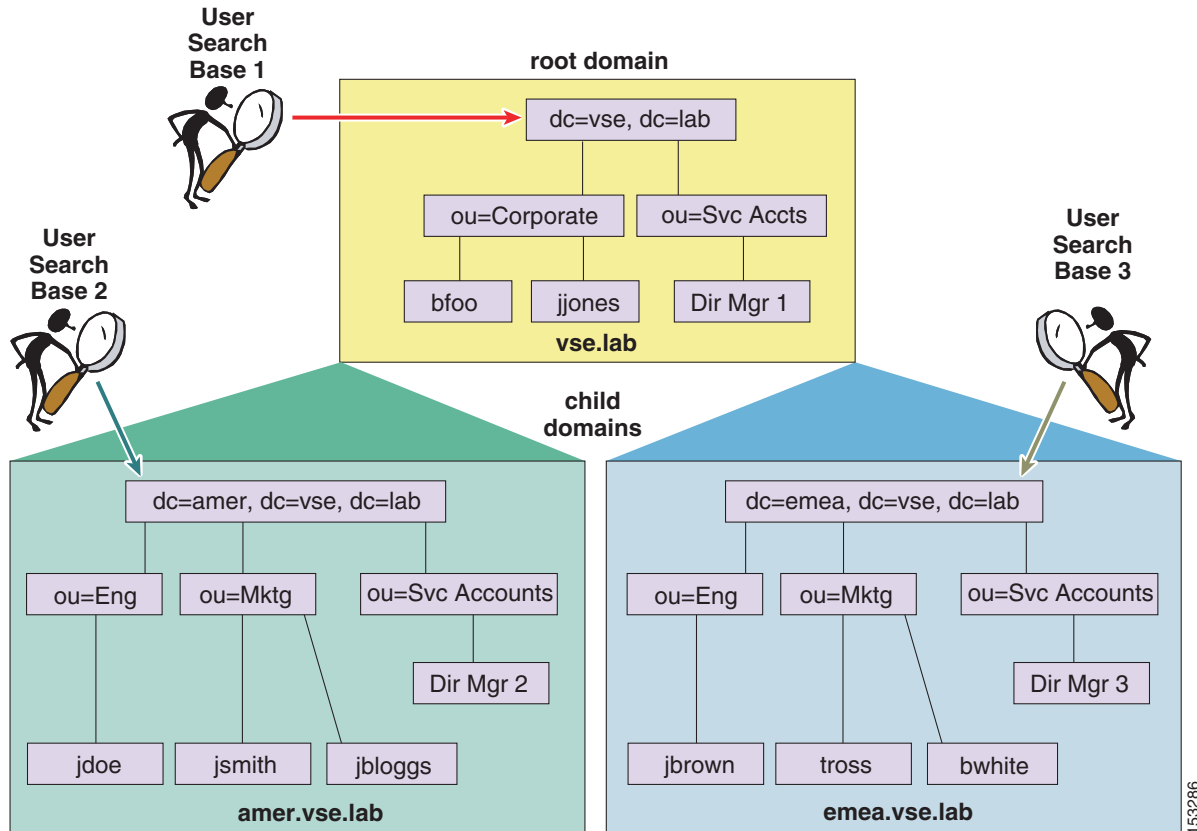
Observe the following design and implementation best practices when deploying LDAP synchronization with Cisco Unified CM 5.x:

- Use a specific account within the corporate directory to allow the Unified CM synchronization agreement to connect and authenticate to it. Cisco recommends that you use an account dedicated to Unified CM, with minimum permissions set to "read" all user objects within the desired search base and with a password set never to expire. (When the password for this account changes in the directory, Unified CM must be reconfigured to take the change into account.)
- All synchronization agreements on a given cluster must integrate with the same family of LDAP servers (either Microsoft AD or Netscape, iPlanet, and Sun ONE).
- Stagger the periodicity of synchronization agreements so that multiple agreements are not querying the same LDAP servers simultaneously. Choose synchronization times that occur during quiet periods.
- If security of user data is of concern, enable Secure LDAP (SLDAP) by checking the **Use SSL** field on the LDAP Directory configuration page in Unified CM Administration.
- Ensure that the LDAP directory attribute chosen to map into the Unified CM UserID field is unique within all synchronization agreements for that cluster.
- The attribute chosen as UserID must not be the same as that for any of the Application Users defined in Unified CM.
- An existing account in the Unified CM database before synchronization is maintained only if an account imported from the LDAP directory has a matching attribute. The attribute that is matched to the Unified CM UserID is determined by the synchronization agreement.
- Configure at least two LDAP servers for redundancy. You can use IP addresses instead of host names to eliminate dependencies on Domain Name System (DNS) availability.
- Administer end-user accounts through the LDAP directory's management tools, and manage the Cisco-specific data for those accounts through the Unified CM Administration web page.

Additional Considerations for Microsoft Active Directory

A synchronization agreement for a domain will not synchronize users outside of that domain nor within a child domain because Unified CM does not follow AD referrals during the synchronization process. The example in [Figure 17-10](#) requires three synchronization agreements to import all of the users. Although Search Base 1 specifies the root of the tree, it will not import users that exist in either of the child domains. Its scope is only VSE.LAB, and separate agreements are configured for the other two domains to import those users.

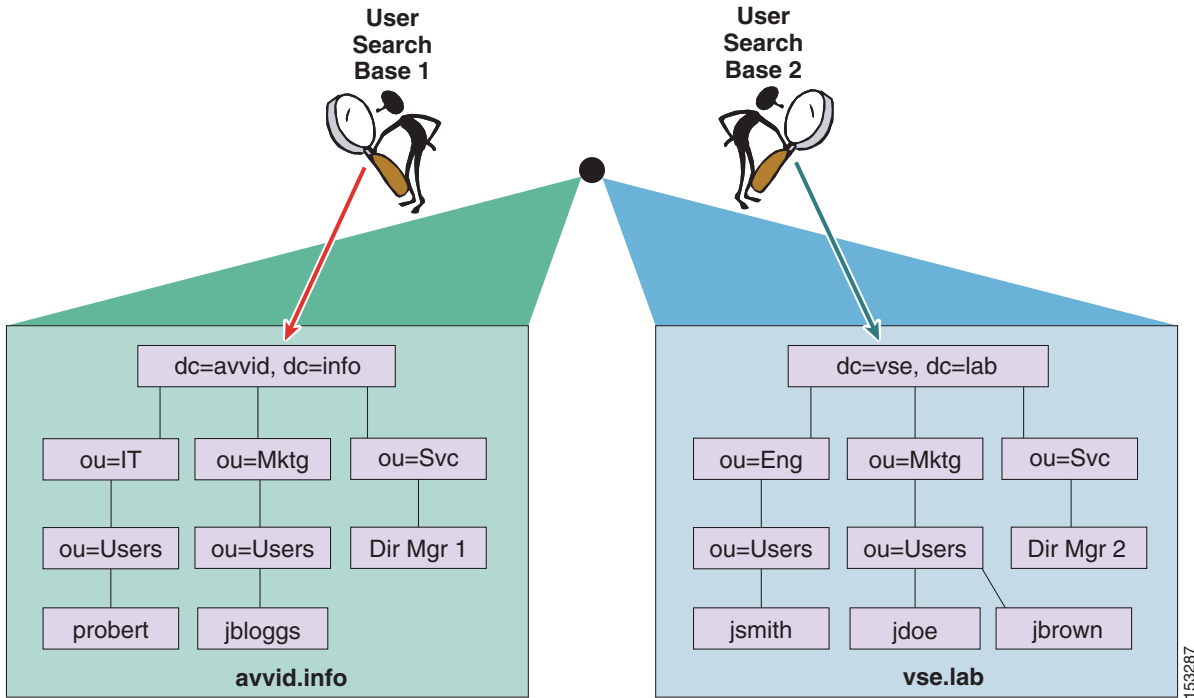
Figure 17-10 Synchronization with Multiple Active Directory Domains



In Figure 17-10, each of the domains and sub-domains contains at least one domain controller (DC) associated to them, and the three synchronization agreements each specify the appropriate domain controller. The DCs have information only on users within the domain where they reside, therefore three synchronization agreements are required to import all of the users.

When synchronization is enabled with an AD forest containing multiple trees, as shown in Figure 17-11, multiple synchronization agreements are still needed for the same reasons listed above. Additionally, the UserPrincipalName (UPN) attribute is guaranteed by Active Directory to be unique across the forest and must be chosen as the attribute that is mapped to the Unified CM UserID. For additional considerations on the use of the UPN attribute in a multi-tree AD scenario, see the section on [Additional Considerations for Microsoft Active Directory](#), page 17-22.

Figure 17-11 Synchronization with Multiple AD Trees (Discontiguous Namespaces)

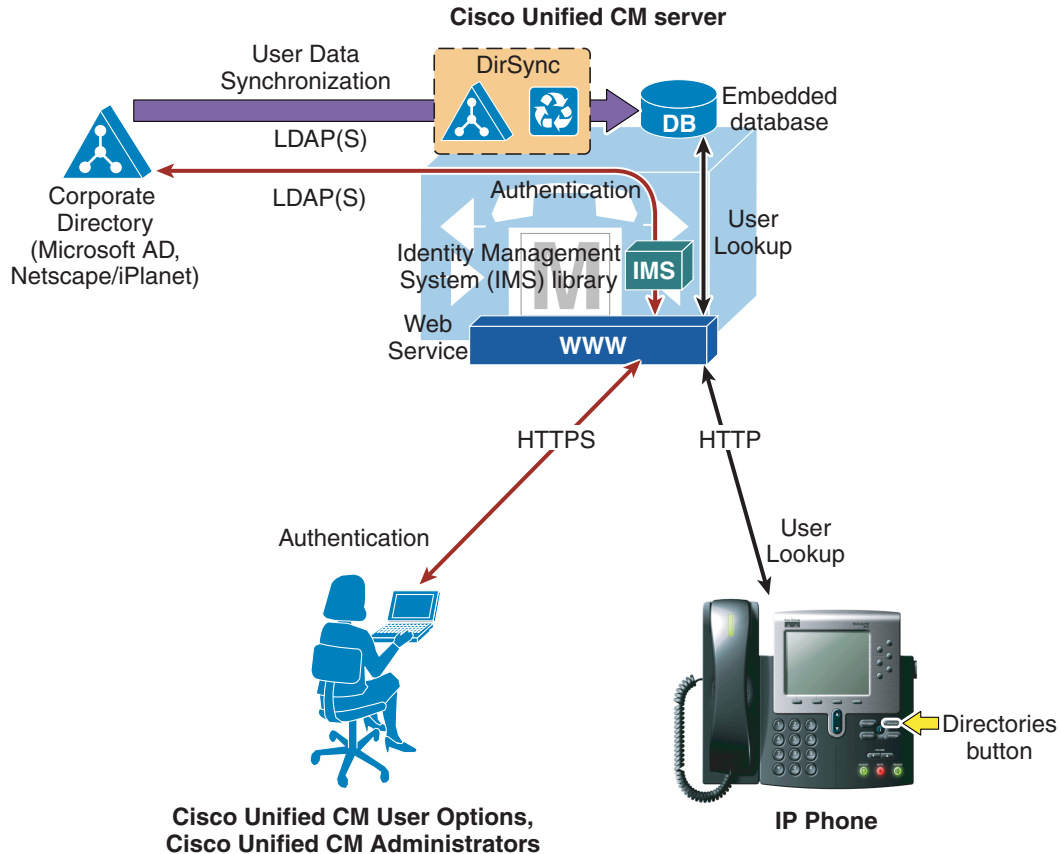


153287

LDAP Authentication

The LDAP authentication feature enables Unified CM to authenticate end user passwords against a corporate LDAP directory instead of using the embedded database. This authentication is accomplished with an LDAPv3 connection established between the IMS module within Unified CM and a corporate directory server, as shown in [Figure 17-12](#).

Figure 17-12 Enabling LDAP Authentication



153288

As in the case of the LDAP synchronization feature, the supported corporate directory products are:

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

To enable authentication, a single authentication agreement may be defined for the entire cluster. The authentication function allows configuration of up to three servers for redundancy, and it also supports secure connections to the directory server if you optionally enable LDAP over SSL (SLDAP). It is not possible to enable the authentication functionality without also enabling the synchronization functionality.

The following statements describe Unified CM's behavior when authentication is enabled:

- End user passwords are authenticated against the corporate directory.
- Application user passwords are authenticated against the Unified CM database.
- End user PINs are authenticated against the Unified CM database.

This behavior is in line with the guiding principle of providing single logon functionality for end users while making the operation of the real-time IP Communications system independent of the availability of the corporate directory, and is shown graphically in Figure 17-13.

Figure 17-13 Authenticating End User Passwords, Application User Passwords, and End User PINs

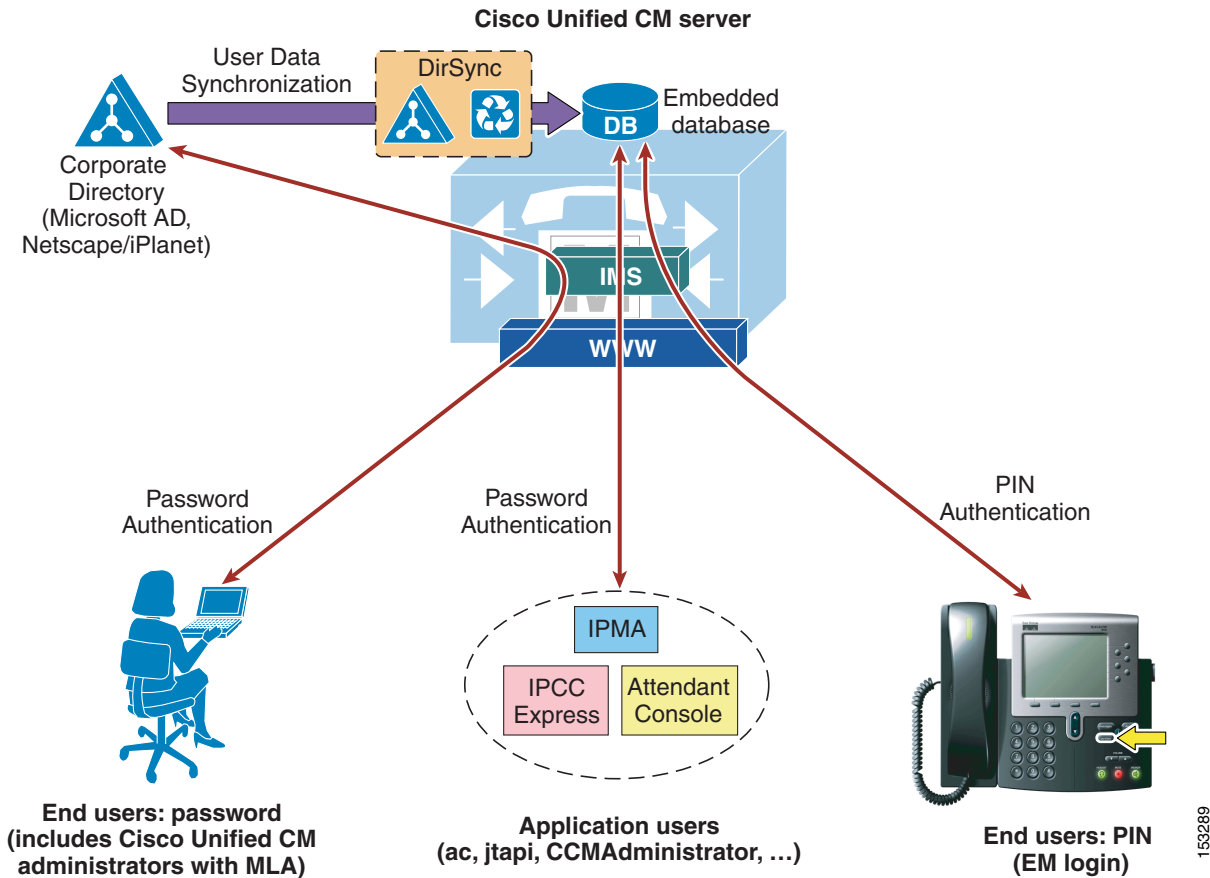
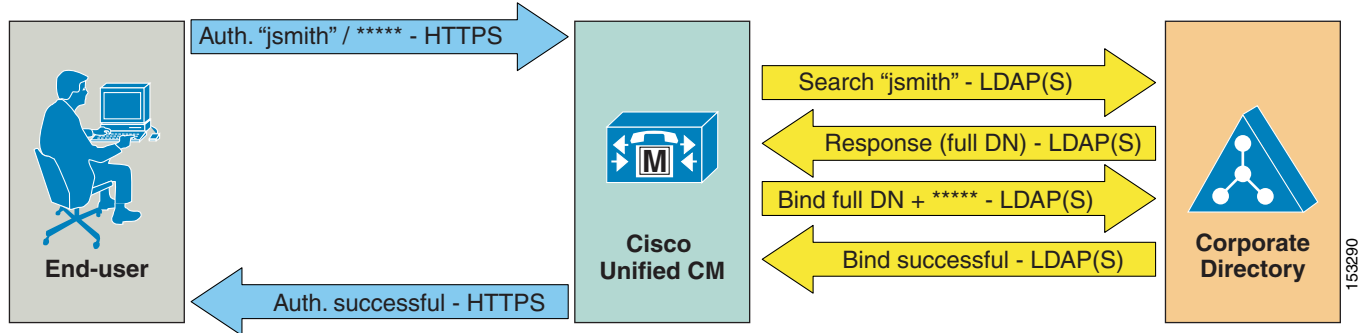


Figure 17-14 illustrates the following process, adopted by Unified CM to authenticate an end user against a corporate LDAP directory:

1. First, a user connects to the Unified CM User Options page via HTTPS and attempts to authenticate with a user name and password. In this example, the user name is jsmith.
2. Unified CM then issues an LDAP query for the user name jsmith, using the value specified in the LDAP Search Base on the LDAP Authentication configuration page as the scope for this query. If SLDAP is enabled, this query travels over an SSL connection.
3. The corporate directory server replies via LDAP with the full Distinguished Name (DN) of user jsmith (for example, "cn=jsmith, ou=Users, dc=vse, dc=lab").
4. Unified CM then attempts an LDAP bind using this full DN and the password provided by the user.
5. If the LDAP bind is successful, Unified CM allows the user to proceed to the configuration page requested.

Figure 17-14 Authentication Process



Observe the following design and implementation best-practices when deploying LDAP authentication with Cisco Unified CM 5.x:

- Create an account within the corporate directory to allow Unified CM to connect and authenticate to it. Cisco recommends that you use an account dedicated to Unified CM, with minimum permissions set to "read" all user objects within the desired search base and with a password set to never expire. (When the password for this account changes in the directory, Unified CM must be reconfigured to take the change into account.) If LDAP synchronization is also enabled, you can use the same account for both functions.
- Enable LDAP authentication on Unified CM by specifying the credentials of the aforementioned account under LDAP Manager Distinguished Name and LDAP Password, and by specifying the directory subtree where all the users reside under LDAP User Search Base.
- Configure at least two LDAP servers for redundancy. You can use IP addresses instead of host names to eliminate dependencies on Domain Name System (DNS) availability.
- This method provides single logon functionality to all end users: when they log in to the Unified CM User Options page, they can now use their corporate directory credentials.
- Manage end user passwords from within the corporate directory interface. (Note that the password field is no longer displayed in the Unified CM Administration pages when authentication is enabled.)
- Manage end user PINs from within Unified CM Administration or from the Unified CM User Options page.
- Manage Application User passwords from within Unified CM Administration. (Remember that these virtual users are only for communication with other Cisco IP Communications functions and applications, and they are not associated with real people.)
- Enable single logon for Unified CM administrators by adding their corresponding end user to the Unified CM Super Users user group from within the Unified CM Administration pages. Multiple levels of administrator rights can be defined by creating customized user groups and roles.

Additional Considerations for Microsoft Active Directory

When you enable LDAP authentication with Microsoft Active Directory, Cisco recommends that you configure Unified CM to query a Microsoft Active Directory Global Catalog server for faster response times.

To enable queries against the Global Catalog, simply configure the LDAP Server Information in the LDAP Authentication page to point to the IP address or host name of a Domain Controller that has the Global Catalog role enabled, and configure the LDAP port as 3268.

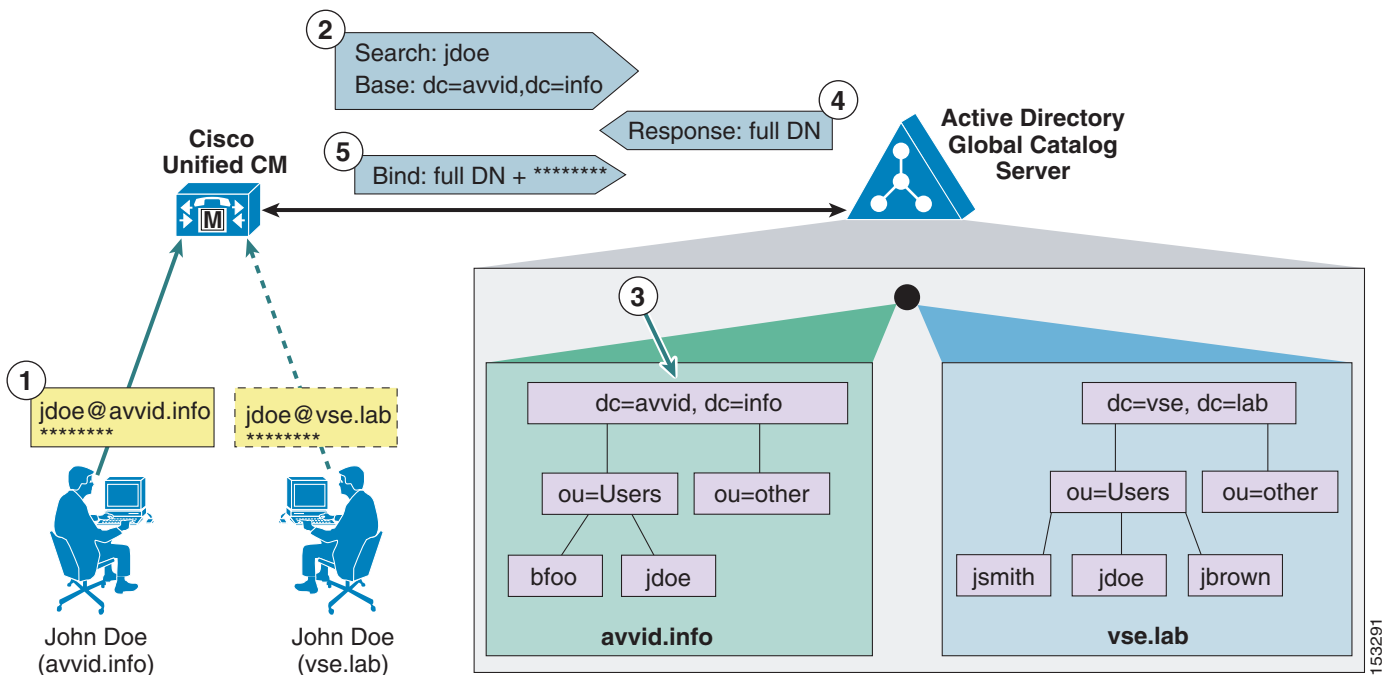
The use of Global Catalog for authentication becomes even more efficient if the users synchronized from Microsoft AD belong to multiple domains, because it allows Unified CM to authenticate users immediately without having to follow referrals. For these cases, point Unified CM to a Global Catalog server and set the LDAP User Search Base to the top of the root domain.

In the case of a Microsoft AD forest that encompasses multiple trees, some additional considerations apply. Because a single LDAP search base cannot cover multiple namespaces, Unified CM must use a different mechanism to authenticate users across these discontinuous namespaces.

As mentioned in the section on [LDAP Synchronization, page 17-11](#), in order to support synchronization with an AD forest that has multiple trees, the UserPrincipalName (UPN) attribute must be used as the user ID within Unified CM. When the user ID is the UPN, the LDAP authentication configuration page within Unified CM Administration does not allow you to enter the LDAP Search Base field, but instead it displays the note, "LDAP user search base is formed using userid information."

In fact, the user search base is derived from the UPN suffix for each user, as shown in [Figure 17-15](#). In this example, a Microsoft Active Directory forest consists of two trees, `avvid.info` and `vse.lab`. Because the same user name may appear in both trees, Unified CM has been configured to use the UPN to uniquely identify users in its database during the synchronization and authentication processes.

Figure 17-15 Authentication with Microsoft AD Forests with Multiple Trees



As shown in [Figure 17-15](#), a user named John Doe exists in both the `avvid.info` tree and the `vse.lab` tree. The following steps illustrate the authentication process for the first user, whose UPN is `jdoe@avvid.info`:

1. The user authenticates to Unified CM via HTTPS with its user name (which corresponds to the UPN) and password.
2. Unified CM performs an LDAP query against a Microsoft Active Directory Global Catalog server, using the user name specified in the UPN (anything before the @ sign) and deriving the LDAP search base from the UPN suffix (anything after the @ sign). In this case, the user name is `jdoe` and the LDAP search base is "`dc=avvid, dc=info`".

3. Microsoft Active Directory identifies the correct Distinguished Name corresponding to the user name in the tree specified by the LDAP query. In this case, "cn=jdoe, ou=Users, dc=avvid, dc=info".
4. Microsoft Active Directory responds via LDAP to Unified CM with the full Distinguished Name for this user.
5. Unified CM attempts an LDAP bind with the Distinguished Name provided and the password initially entered by the user, and the authentication process then continues as in the standard case shown in [Figure 17-14](#).

**Note**

Support for LDAP authentication with Microsoft AD forests containing multiple trees relies exclusively on the approach described above. Therefore, support is limited to deployments where the UPN suffix of a user corresponds to the root domain of the tree where the user resides. If the UPN suffix is disjointed from the actual namespace of the tree, it is not possible to authenticate Unified CM users against the entire Microsoft Active Directory forest. (It is, however, still possible to use a different attribute as user ID and limit the integration to a single tree within the forest.)

User Filtering for Directory Synchronization and Authentication

This section describes the LDAP Query Filter mechanism available in Cisco Unified CM 5.0 and later. To optimize directory synchronization performance, Cisco recommends importing only those directory user accounts that will be assigned IP telephony resources from Unified CM. In many cases, a unique search base is all that is needed. When a unique search base is not available, a custom LDAP filter might be required. The information in the following sections addresses both methods that can be used to optimize directory synchronization.

Optimizing Unified CM Database Synchronization

The Unified CM Database Synchronization feature provides a mechanism for importing a subset of the user configuration data (attributes) from the LDAP store into the Unified CM publisher database. Once synchronization of a user account has occurred, the copy of each user's LDAP account information may then be associated to additional data required to enable specific IP communication features for that user. When authentication is also enabled, the user's credentials are used to bind to the LDAP store for password verification. The end user's password is never stored in the Unified CM database when enabled for synchronization and/or authentication.

User account information is cluster-specific. Each Unified CM publisher server maintains a unique list of those users receiving IP telephony services from that cluster. Synchronization agreements are cluster-specific, and each publisher has its own unique copy of user account information.

Only those users who will be assigned IP telephony resources should be synchronized with Unified CM. The following is a partial list of common reasons why the entire set of users defined in the LDAP directory should not be imported into the Unified CM cluster:

- Importing users who will not be assigned IP telephony resources can increase directory synchronization time.
- Importing users who will not be assigned IP telephony resources can slow Unified CM searches and overall database performance.

- In many cases, the number of user accounts in the LDAP store far exceeds the total user capacity of the Unified CM cluster. Limit synchronization of users to reflect the recommended limits for specific software and hardware combinations as listed in the Cisco Unified CM Release Notes, available at

<http://www.cisco.com>

Unified CM has no enforced limit on the number of accounts that may be added to the system. In all cases, Cisco recommends limiting the number of users to the same quantity as the supported number of endpoints. For example, a full-sized cluster of Cisco MCS-7845 servers can support up to 30,000 endpoints, and the system should be administered to limit the number of users to roughly 30,000. There might be cases where accounts are needed for applications, and some designs might require additional accounts.

Cisco recommends using the control mechanisms described here to minimize the number of user accounts imported, regardless of the LDAP database size. This will improve the speed of the first and subsequent periodic synchronizations and will also improve manageability of the user accounts.

Using the LDAP Structure to Control Synchronization

Many deployments of LDAP directories use the Organizational Unit Name (OU) to organize users into some logical grouping. If the LDAP directory has a structure that organizes users into multiple OUs, then it often is possible to use that structure to control which users are imported. Each individual Unified CM synchronization agreement specifies a single OU. Only those users in the OU are synchronized. When multiple OUs containing users are required in a cluster, then multiple synchronization agreements are required. When an OU contains users that will *not* be assigned IP telephony resources, then Cisco recommends omitting those OUs from the directory synchronization.

