CHAPTER 18

LDAP Directory Integration

Last revised on: February 13, 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 CallManager 4.*x* with a corporate LDAP directory. The main topics include:

- What is Directory Integration?, page 18-2

  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 18-3

  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 Cisco Unified CallManager 4.x, page 18-6

  This section describes the technical solutions and provides design best-practices for directory integration with Cisco Unified CallManager 4.*x*.

The considerations presented in this chapter apply to Cisco Unified CallManager 4.*x* as well as the following applications bundled with it: Extension Mobility, Cisco Unified CallManager Assistant, WebDialer, Bulk Administration Tool, and Real-Time Monitoring Tool.

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

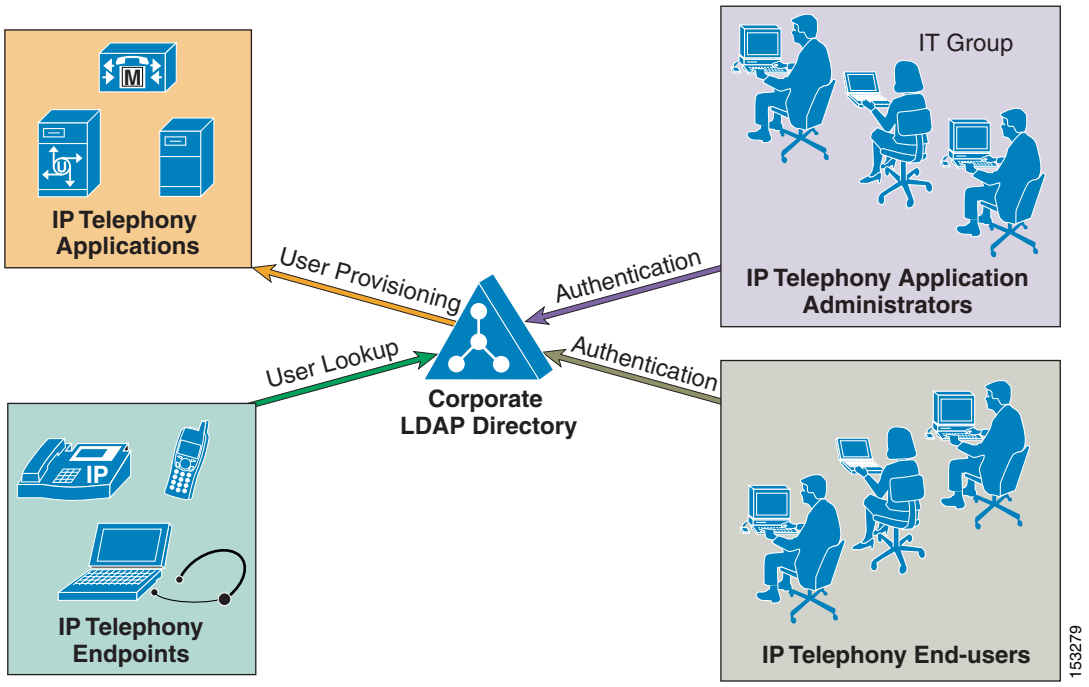
For Cisco Unity, refer to the *Cisco Unity Design Guide* and to the following white papers: *Cisco Unity Data and the Directory*, *Active Directory Capacity Planning*, and *Cisco Unity Data Architecture and How Cisco Unity Works*, also available at

http://www.cisco.com

What 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 18-1.

Figure 18-1 Various Requirements for Directory Integration



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 Cisco Unified CallManager version used, as summarized in Table 18-1.

Table 18-1 Directory Requirements and Cisco Solutions

Requirement	Cisco Solution	Cisco Unified CallManager 4.*x* Feature	Cisco Unified CallManager 5.0 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
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 18-1, 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 CallManager Release 4.*x*. For a detailed description of directory integration solutions with Cisco Unified Communications Manager Release 5.*x*, refer to the *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 5.x*, available at

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

Directory Access for IP Telephony Endpoints

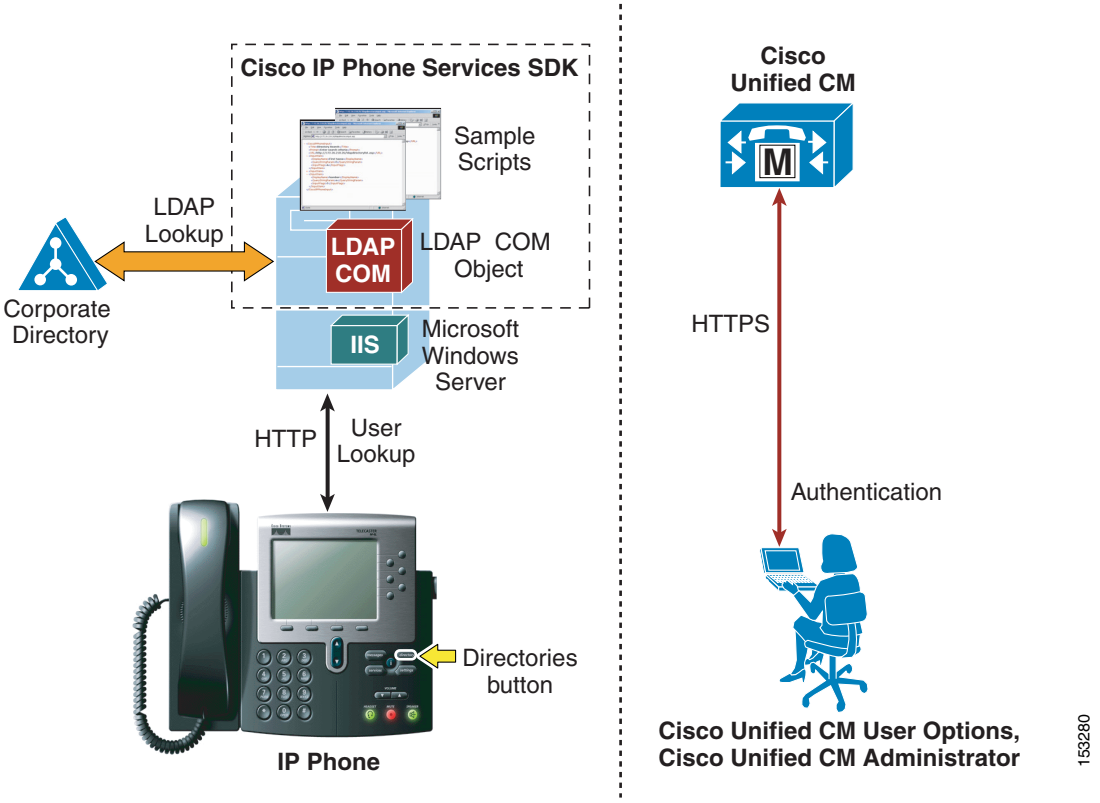
This section describes how to configure corporate directory access to any LDAP-compliant directory server to perform user lookups from Cisco Unified Communications endpoints (such as Cisco Unified IP Phones). The guidelines contained in this section apply regardless of whether Cisco Unified CallManager 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 Cisco Unified CallManager'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 18-2 illustrates this mechanism in a deployment where Cisco Unified CallManager has not been integrated with the corporate directory. Note that, in this scenario, Cisco Unified CallManager is not involved in the message exchange related to the user lookup.

Figure 18-2 Directory Access for Cisco Unified IP Phones Using the Cisco Unified IP Phone Services SDK



In the example shown in Figure 18-2, 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 Cisco Unified CallManager 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 Cisco Unified CallManager, 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 Cisco Unified CallManager 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 Cisco Unified CallManager users with the corporate directory.

Directory Integration with Cisco Unified CallManager 4.*x*

This section describes the mechanisms and best practices for directory integration with Cisco Unified CallManager 4.*x* to allow for user provisioning and authentication with a corporate LDAP directory. This section covers the following topics:

Cisco Unified CallManager 4.*x* Directory Architecture

Cisco Unified CallManager 4.*x* uses an embedded Microsoft SQL database to store system and device configuration data, such as dial plan information, phone and gateway configurations, and media resource utilization. It also uses an embedded LDAP directory to store user and application profiles, such as devices controlled by a user, computer telephony integration (CTI) user parameters, and personal address book entries.

Both the SQL database and the LDAP directory run on every Cisco Unified CallManager 4.*x* server within a cluster, and replication agreements are automatically set up between servers. The publisher server contains the master copy of both the SQL database and the LDAP directory, and it handles replication to all subscriber servers, which contain read-only copies of both repositories.

Note The examples and recommendations in this chapter are based on Cisco Unified CallManager 4.*x*, which introduced some new features and enhancements. Some behaviors might differ and some features might not be available if you are running an older version of Cisco CallManager.

To store application-specific information in an LDAP directory, Cisco Unified CallManager 4.*x* adopts an approach that is valid both when using the embedded directory and when integrating with a corporate directory.

Cisco Unified CallManager utilizes a subset of the Cisco registered object identifies (OIDs) when it extends the schema. The OID values are 1.2.840.113548.3.1.4.*xx* for attributes and 1.2.840.113548.3.2.4.*xx* for object classes.

Because different directory vendors typically use different User object models with several additional, nonstandard attributes, Cisco Unified CallManager 4.*x* uses only the standard LDAPv3 core attributes from the User object. The User object is then augmented with an auxiliary class, ciscoocUser, which contains the following attributes:

- ciscoatGUID

  This attribute uniquely identifies a user within the directory.

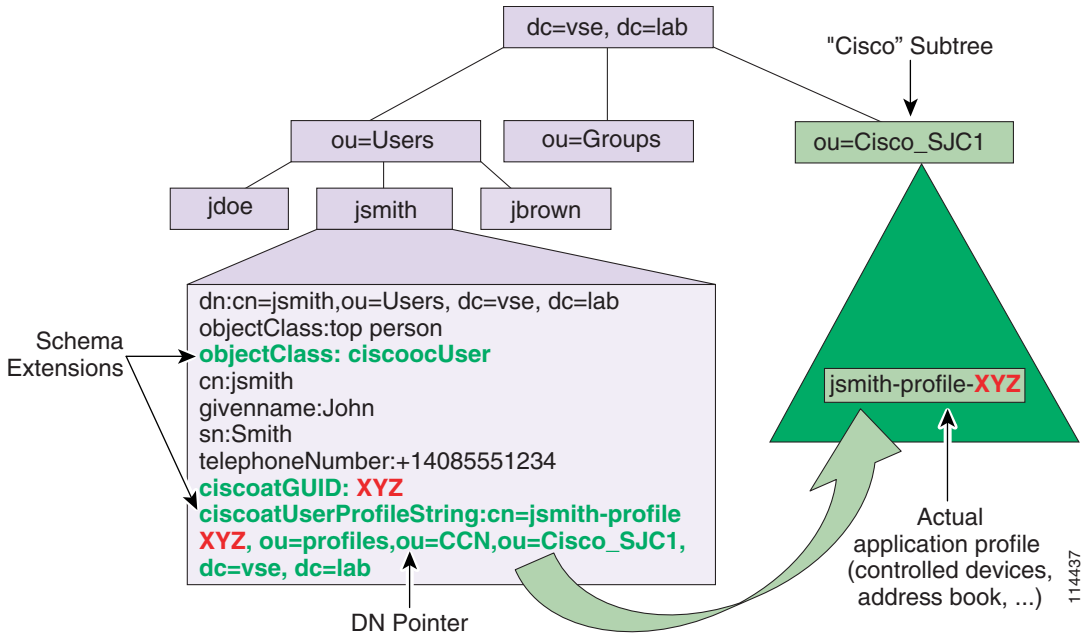
- ciscoatUserProfile

  This attribute is used by earlier versions of Cisco Unified CallManager 4.*x* and other applications. It is still present for backward compatibility.

- ciscoatUserProfileString

  This attribute is a distinguished name pointer to another object in the directory, which contains the user's application-specific profile. This approach minimizes the impact on the core User object, and all the application-specific information can be stored in a separate organizational unit (OU) within the directory, usually called the Cisco subtree, CISCOBASE, or Cisco Directory Information Tree (DIT). Figure 18-3 illustrates this process.

Figure 18-3 Approach to Storing Application-Specific User Information in the Directory with Cisco Unified CallManager 4.x



The object pointed to by the ciscoatUserProfileString attribute belongs to a structural object class called ciscoocUserProfile. The main purpose of this object is to store some specific details for the user, including the user's locale, any Cisco IP Manager Assistant (IPMA) assistants for the user, and pointers to various specific profile objects for all Cisco applications that integrate with the directory. The application profile used by Cisco Unified CallManager 4.*x* belongs to the auxiliary class called ciscoCCNocAppProfile, and it is where Cisco Unified CallManager 4.*x* stores the user's extension mobility PIN, the list of devices controlled by this user, information on whether this user is permitted to use CTI applications, and so on. Both of these profile objects are created by Cisco Unified CallManager 4.*x* under the "Cisco" subtree.

Note The list of devices associated with a user is stored in the directory as a multi-valued attribute. If you are using the embedded Cisco Unified CallManager 4.*x* directory (known as DC Directory), the maximum number of devices that can be associated with a user is 2,000 (or 2,500 if all subscribers in the cluster are dual-CPU servers). However, Microsoft Active Directory limits the number of values that can be stored in a multi-valued attribute. The total size of the record should never exceed 7,000 bytes, which allows for approximately 850 attribute values.

If you are integrating Cisco Unified CallManager 4.*x* with Microsoft Active Directory (AD), use the following method to calculate the maximum number of devices, device profiles, or combination of both that can be associated with a single user:

Total record size = 9 * (Total number of devices associated with a user) + (Size in bytes of the name of each associated device profile).

This calculated record size must be less than 7,000 bytes.

The following examples illustrate the use of this calculation method.

Example 18-1 Devices Only (Device Profiles Not Used)

Number of devices = 500.

Total record size = 9 * 500 = 4,500 bytes.

Because the calculated record size is less than 7,000, this user's device associations are within the acceptable limit for AD.

Example 18-2 Devices and Device Profiles

Number of devices = 400.

Number of device profiles = 339.

Each profile name is 10 characters (bytes).

Total record size = (9 * 400) + (339 * 10) = 3600 + 3390 = 6,990 bytes.

Because the calculated record size is less than 7,000, this user's device associations are within the acceptable limit for AD.

The total number of associations for this user = 400 + 339 = 739.

Example 18-3 Devices and Device Profiles

Number of devices = 400.

Number of device profiles = 400.

Each profile name is 10 characters (bytes).

Total record size = (9 * 400) + (400 * 10) = 3600 + 4000 = 7,600 bytes.

This user's device associations exceed the limit of 7,000 bytes and would not be an acceptable directory entry in AD. To bring this user's device associations within the record size limit for AD, reduce the number of devices and device profiles associated with this user.

The Cisco Customer Directory Configuration Plugin

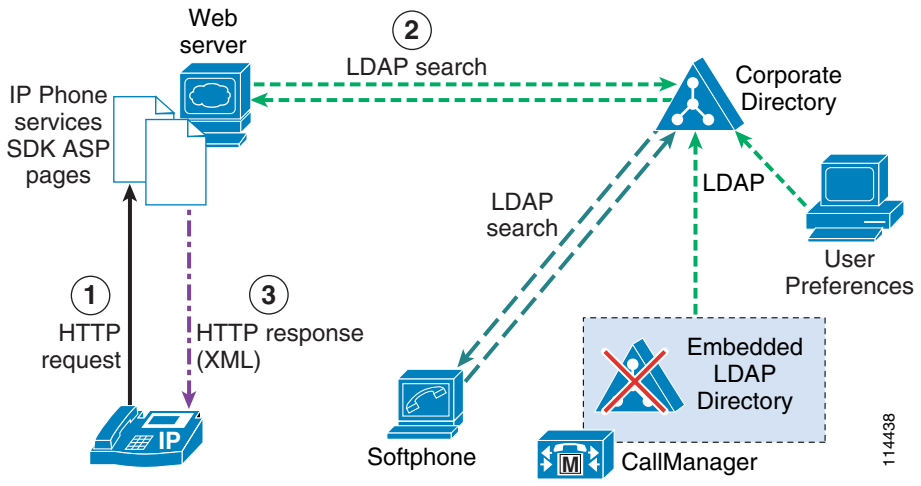
To integrate Cisco Unified CallManager with an external LDAP directory, run the Cisco Customer Directory Configuration Plugin, which is bundled with Cisco Unified CallManager (**Applications > Install Plugins**). This plugin serves three main purposes:

- It extends the corporate directory schema to accommodate the application-specific objects and attributes.
- It populates the "Cisco" subtree with the configuration objects needed by Cisco Unified CallManager.
- It configures Cisco Unified CallManager to use the corporate directory and disables its embedded directory.

Usually, running the plugin locally on Cisco Unified CallManager performs the schema update. However, starting with Cisco Unified CallManager Release 4.0, a new option exists to create the LDAP Data Interchange Format (LDIF) files separately so that the schema update can be performed directly on the corporate directory's Schema Master server using the LDIF files. This option allows different groups of people to perform the relevant parts of the work and reduces the need to update over the network when Cisco Unified CallManager is not local to the Schema Master server.

After the plugin has been run, Cisco Unified CallManager effectively uses the corporate directory to store user preferences. If the Cisco IP Telephony endpoints have also been enabled to access the corporate directory, as described in the preceding section, the resulting scenario is that shown in Figure 18-4.

Figure 18-4 Message Exchange for Cisco IP Phone Corporate Directory Access When Cisco Unified CallManager Is Integrated with the Corporate Directory



Security Considerations

Starting with Cisco Unified CallManager Release 4.1, the communication between Cisco Unified CallManager and the embedded directory is set by default to use LDAP over Secure Socket Layer (SSL), also known as LDAPS.

When integrating with a corporate directory, it is also possible to enable LDAP over SSL, thus ensuring that all sensitive LDAP data goes over a secure connection. The LDAP over SSL option can be configured as part of the Cisco Customer Directory Plugin, and it requires a certificate shared with the corporate directory and issued by the same Certificate Authority.

When LDAP over SSL is enabled for Cisco Unified CallManager, the following additional Cisco IP Communications applications will also communicate with the directory over this secure channel:

- User pages within Cisco Unified CallManager Administration
- Cisco Multi-Level Administration (MLA)
- Cisco IP Phone Options pages
- Extension Mobility application — SSL is used for communications between the Extension Mobility application, running on a Cisco Unified CallManager server, and the corporate directory. However, SSL is not used for communications between the IP phones and the Extension Mobility application, which use HTTP instead.
- Cisco CTI Manager
- Serviceability and Cisco Real-Time Monitoring Tool (RTMT)
- Cisco CDR Analysis and Reporting (CAR)
- Cisco IP Manager Assistant (IPMA) service
- Cisco Bulk Administration Tool (BAT)

Multilevel Administration Account Security

Prior to Cisco Unified CallManager Release 4.2, the Multilevel Administration (MLA) function performed caching of the authentication status of users that had an MLA association. When MLA was integrated with an off-cluster Microsoft Active Directory (AD), the directory's password security features (such as password aging) could cause interruption of correct MLA functionality. In Cisco Unified CallManager 4.2, a new set of controls was added to allow control over the caching function of MLA so that it would not be affected by these password security features.

The password caching can allow a user to authenticate successfully in some instances when the directory has disabled or otherwise blocked an account since the cache entry was made. The new feature also avoids this behavior.

In Cisco Unified CallManager 4.2, the User Cache Flush Timeout parameter is enabled with a default value of 5 minutes. The parameter determines the lifetime of the cached authentication status. The AVVID XML Layer (AXL) and Simple Object Access Protocol (SOAP) interfaces on Cisco Unified CallManager are also affected by this parameter because they use the same authentication mechanism as MLA. The parameter for caching can be set to disable caching. When using applications enabled for SOAP or AXL, be aware that their performance will be impacted because they are usually polling-type applications that require frequent authentication. Therefore, Cisco recommends that you do *not* disable the caching.

Adding Cisco Unified CallManager Servers to a Domain

Adding the Cisco Unified CallManager servers to a Microsoft Windows domain differs substantially from integrating Cisco Unified CallManager with an external directory. Although these operations do not exclude each other, they are completely independent and have different implications:

- Adding Cisco Unified CallManager servers to a Microsoft Windows Active Directory (AD) domain could cause domain policies to be applied to the Windows 2000 Server operating system, and the addition affects only the management of the Cisco Unified CallManager server itself.
- Integrating Cisco Unified CallManager with an external directory (such as Microsoft Active Directory or Netscape Directory Server) causes Cisco Unified CallManager to store all its user information and preferences in that directory, but it does not affect management of the Cisco Unified CallManager server itself.

Cisco recommends that you keep Cisco Unified CallManager servers as workgroup servers. However, if you want to add the servers to a domain, avoid applying domain policies to the server that could interfere with its normal operation.

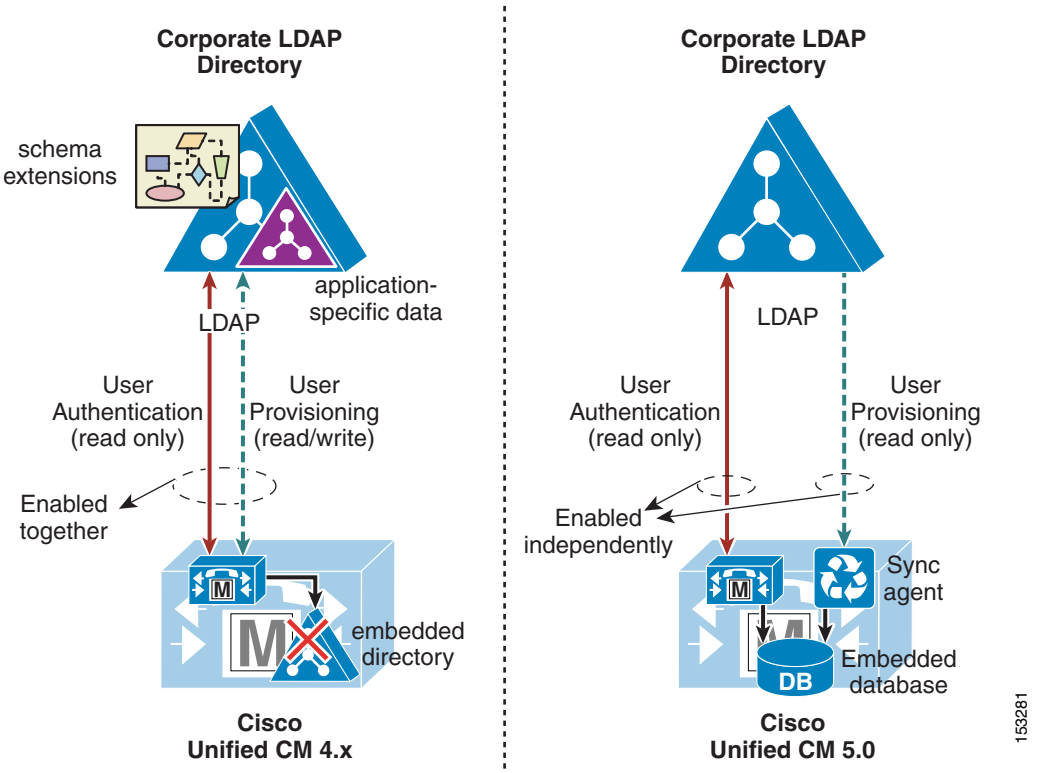
For additional recommendations about adding servers to a domain, refer to the latest Cisco Unified CallManager product documentation available online at

http://www.cisco.com

Comparison with the Cisco Unified CallManager 5.0 Approach

The approach to directory integration changes significantly with Cisco Unified CallManager Release 5.0, and this section highlights the main differences with the current Cisco Unified CallManager 4.*x* approach. Figure 18-5 shows high-level functional diagrams of the two approaches to achieve user provisioning and authentication.

Figure 18-5 Directory Integration Approaches in Cisco Unified CallManager 4.x and 5.0



Cisco Unified CallManager Release 4.*x* uses an embedded LDAP directory to store user-related information. Directory integration is 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 is effectively used as the back-end storage repository for user information, this method satisfies the requirement for both user provisioning and user authentication. Any changes to user data in the corporate directory are immediately picked up by Cisco Unified CallManager because it accesses the same data store.

However, this approach has an impact on the corporate directory in terms of schema extensions and additional data, and it also introduces dependencies between the real-time functionality of the IP Communications system and the availability of the directory. When connectivity is lost or the directory becomes unavailable, Cisco Unified CallManager is unable to access all user-related configurations, which impacts applications such as Extension Mobility, Attendant Console, and IP Contact Center Express. In this approach, the user provisioning and user authentication functions have to be enabled at the same time because they rely on the same integration process. In addition, using the corporate directory as the storage repository for application-specific data also imposes limitations on the day-to-day maintenance operations on the corporate directory itself, as described in the remainder of this chapter.

By contrast, the approach to directory integration adopted by Cisco Unified CallManager Release 5.0 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 Cisco Unified CallManager 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.

For more information on directory integration with Cisco Unified Communications Manager 5.*x*, refer to the *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 5.x*, available on Cisco.com at

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

Best Practices for Directory Integration

The directory integration process involves several components and services in your network and therefore should be carefully planned and implemented. This section addresses following topics:

- Planning the Directory Integration, page 18-13
- Preparing the Directory for Integration, page 18-15
- Integrating Cisco Unified CallManager with the Directory, page 18-19
- Maintaining the Directory Integration, page 18-22

Note Because the majority of known Cisco Unified CallManager integrations are performed with Microsoft Active Directory (AD), this chapter focuses on best practices for AD. However, most recommendations and best practices mentioned in this section also apply to the other directory product supported by Cisco Unified CallManager, the Sun/iPlanet Netscape Directory Server.

Planning the Directory Integration

Because the directory is an enterprise-wide resource that is used by a potentially large number of applications and end users, it is essential to plan the integration carefully to minimize the impact on all other applications.

Tip Before starting the integration, ensure that your organization's directory team is involved in the planning, design, and implementation phases.

As mentioned previously in this chapter, integrating Cisco Unified CallManager and other applications with an external directory involves extending the directory schema. Schema extension is a delicate operation. For example, in the case of Microsoft Windows 2000 Active Directory, schema changes cannot be undone. You should take the following precautions to avoid damaging the directory:

- Review the planned schema changes with your organization's directory team. This practice should be part of your organization's change control procedures.
- Create a replica of the production directory in a lab setup, and test the integration against it.
- Back up the production directory, both data as well as schema, before integration, and make sure a workable back-out plan exists to enable successful restoration of the data and schema if it becomes necessary.
- Plan and perform the schema extension during off-peak hours to minimize the impact on other applications and end users.

Although the preceding list of precautions might cause concern at first, in practice the schema extension rarely causes problems that would require it to be backed out. However, no matter how safe an operation is known to be, you should not add risk by skipping any possible precautions to ensure that you can recover from unplanned issues.

Another important consideration is that, as soon as the voice applications have been integrated with the directory, they rely on it for their correct operation, and inability to reach the directory server can negatively affect the voice system.

For example, if the directory suddenly becomes unavailable, end users cannot log into the Cisco Unified CallManager User Options web page to configure their preferences; Extension Mobility users, Attendant Console operators, and Unified Contact Center Express agents cannot log in or out; and the dial-by-name function is unavailable.

To avoid these problems, you should design your directory infrastructure so that it is highly available to all Cisco voice applications. You can use any of the following methods to achieve this high availability:

- Leverage the directory replication mechanism to place a directory server or servers in the same location as the Cisco voice applications.
- Use a server load-balancing mechanism, such as Cisco IOS software server load balancing (SLB), to provide server redundancy in a specific campus or data center and to ensure that local servers are accessed by preference.
- Use Domain Name System (DNS) domain names instead of specific domain controller host names when configuring the directory plugin.

With redundant servers, the first name returned by DNS might be the name of a server that is not as local to Cisco Unified CallManager as others returned later in the response. Also, if your DNS server has the round-robin feature enabled, by design it rotates the order in which addresses are returned in the response. Depending on mechanisms such as client-side DNS cache timeout, along with other possible clients querying for the same domain in the interim, Cisco Unified CallManager could run two consecutive operations against two different domain controllers (DCs). In addition to the locality problem already mentioned, using DNS redundancy could keep objects created in the first operation from being found by a search on a different DC by a later query if the directory has not replicated in the meantime. Therefore, before choosing to use DNS to make the implementation redundant, be sure that these issues do not affect your deployment.

Also note that DNS is needed for proper LDAP referral; Cisco Unified CallManager must be able to resolve the host names of any of the DCs returned in an LDAP referral.

Note Although Microsoft Windows 2000 DNS has a feature that returns local resources first (called LocalNetPriority), it is based on inspecting the requesting client's classful IP address. Therefore, it is of limited use in subnetted networks. Microsoft Knowledge Base article 177883 documents this feature (see http://support.microsoft.com/). If you are not using Windows 2000 DNS, you should check to see which features in your chosen implementation might alleviate some of these issues. These recommendations are based on the assumptions that Cisco Unified CallManager is set to use DNS and that it is the same DNS infrastructure used by your Active Directory.

Preparing the Directory for Integration

With Microsoft Windows 2000 Active Directory, the domain controllers have to be set to allow schema changes. This requirement applies only to the domain controller that acts as the Schema Master (the location where change takes place), and it is fully documented in Microsoft Knowledge Base article 285172, which is available at

http://support.microsoft.com

If you are integrating Cisco Unified CallManager with the Microsoft Windows 2000 Active Directory, and if Microsoft Exchange 2000 needs to coexist in the same forest, you must perform an additional preparation step. Cisco Unified CallManager uses the labeledURI attribute specified by the iNetOrgPerson class, as defined in RFC 2798. Microsoft currently defines this attribute differently for Exchange 2000, which causes a naming clash with the Cisco Unified CallManager schema. The problem is documented in Microsoft Knowledge Base article 314649 (available from http://support.microsoft.com). You can obtain the iNetOrgPerson kit from

http://msdn.microsoft.com/en-us/library/ms808546.aspx

Caution Remember to back up your directory before extending the schema. Make sure you have tested the restore mechanism you intend to use *before* you need it.

To extend the directory schema for Cisco Unified CallManager, run the Cisco Customer Directory Configuration plugin from the publisher server for the cluster, and follow these best practices:

- Always use the **Custom** setup type when running the plugin. The Express setup type is appropriate only for integration with a standalone domain used exclusively for Cisco Unified CallManager and other Cisco voice applications. You should never use the Express setup when integrating with an existing domain.
- Select only the **Install Schema on the Schema Master** option in the plugin configuration screen.
- Try to ensure that the Schema Master server is relatively local to Cisco Unified CallManager or that a high-speed connection exists between them. If neither is possible, then consider creating just the LDIF files with the plugin and using them directly to update the schema on the Schema Master.
- In this phase, provide the plugin with credentials (distinguished name and password) for a user who is a member of the Schema Admins group in Active Directory. These credentials are used only for the schema extension, not for normal Cisco Unified CallManager operation.

Note If you have a large AD forest or a complex topology, schema changes might take some time to propagate to all domains and all domain controllers in the forest. Allow enough time for this propagation to happen before continuing with the preparation process, or else force replication if required.

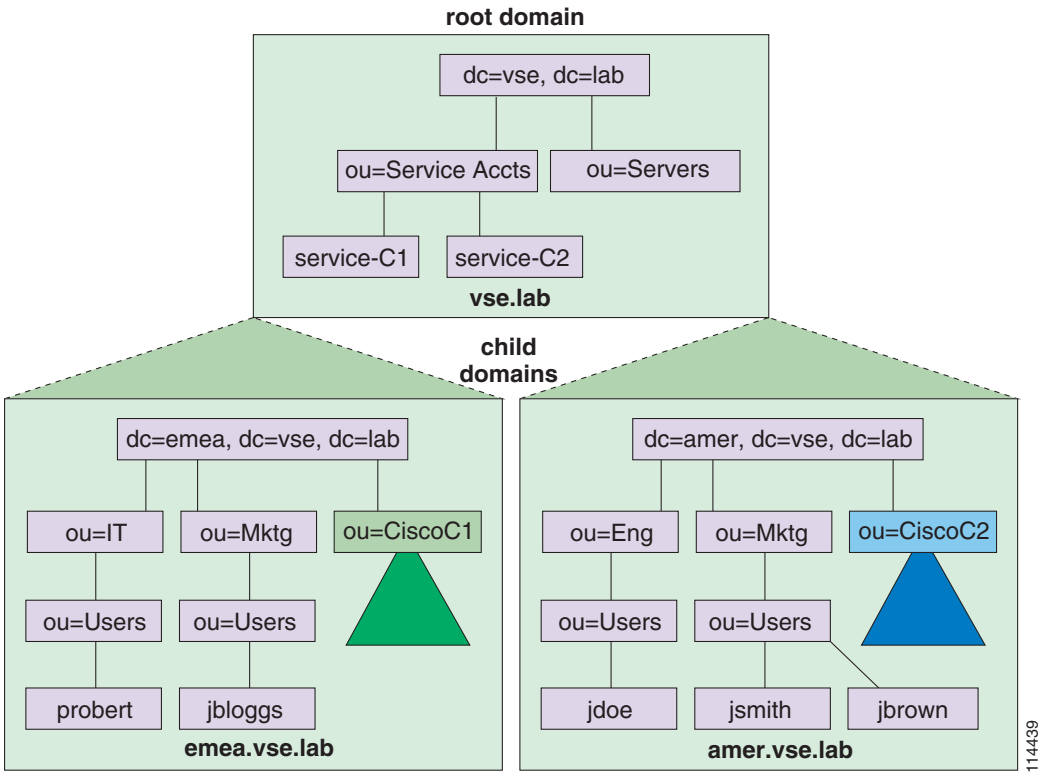
As soon as the schema has been extended, you can decide where to create the "Cisco" OUs (that is, the subtrees) that will be used by the Cisco Unified CallManager clusters and the other Cisco voice applications. There must be one organizational unit (OU) for each Cisco Unified CallManager cluster to be integrated.

For a deployment with a single domain AD or Netscape directory server, placement is not critical. The OU can effectively be placed anywhere in the tree.

In a multiple-domain AD forest, the root domain is often kept free of users and resources and is used as a placeholder domain, so the "Cisco" subtrees would typically reside in the child domains. In this type of multiple-domain topology, domains can be created based on geographic boundaries. Therefore, it is unlikely that every location has a local domain controller for each domain. To reduce replication traffic across the network, domain controllers are usually placed only where needed. With this in mind, it is best to try to place the Cisco OU for a given cluster in the domain containing the majority of users serviced by that cluster.

Figure 18-6 shows a multiple-domain, single-tree AD forest in which the "Cisco" OUs for two Unified CallManager clusters have been created in the two respective child domains, emea.vse.lab and amer.vse.lab.

Figure 18-6 Multiple-Domain, Single-Tree AD Forest

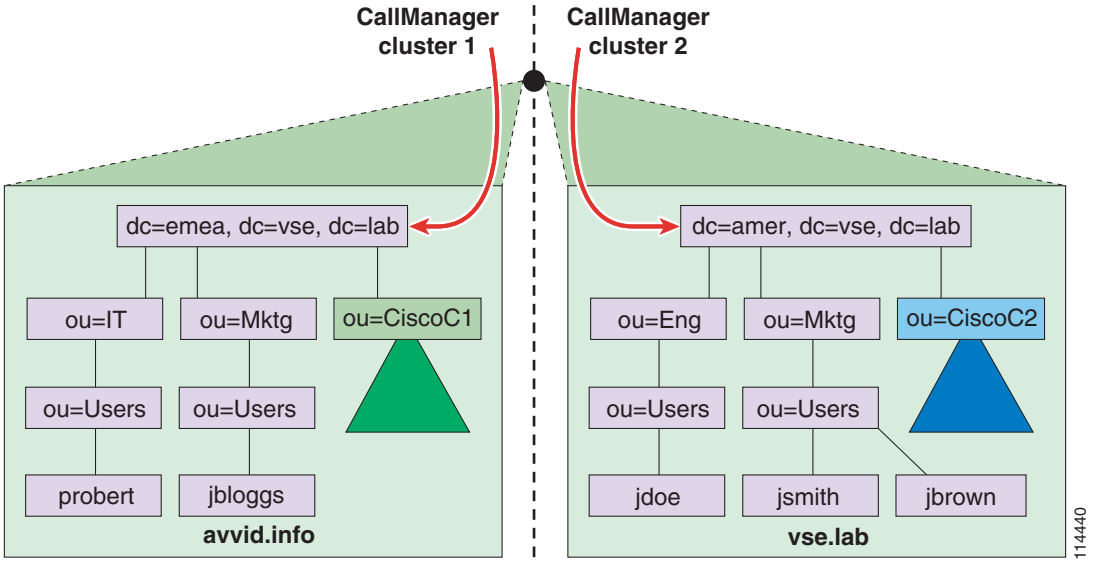


In Figure 18-6, each cluster services the corresponding geography in a centralized call processing model, thus ensuring that its user data stored in AD is also local. This design saves having to retrieve the information from a DC that is probably non-local, and it reduces the number of LDAP referrals required to find the relevant information in a search.

Cisco does not recommend having a Cisco Unified CallManager cluster service users in different domains because response times while user data is being retrieved might be less than optimal if domain controllers for all included domains are not local. However, this scenario is not a common one because the reasons for creating a multiple-domain AD (namely, geography, bandwidth, or organizational structure) are usually the same reasons for needing multiple clusters.

Currently clusters cannot span trees within an AD forest because they would not have a contiguous namespace, which is a requirement for LDAP referrals. A cluster can exist within a domain or a single tree, even in a multiple-tree forest (as described previously), but all the users for a specific cluster must be contained in the same namespace, as shown in Figure 18-7.

Figure 18-7 Cisco Unified CallManager Clusters Must Be Contained Within a Single Tree (Contiguous Namespace)



The User Search Base is another important element used by Cisco Unified CallManager when integrating with a directory. The User Search Base refers to the root of the subtree used by Cisco Unified CallManager to search for users who can potentially be associated with devices within the cluster. (The section on Integrating Cisco Unified CallManager with the Directory, page 18-19, discusses how to set this parameter.)

You should create a special user account that Cisco Unified CallManager and the other Cisco voice applications can use to access and manage the directory. There should be one account per Cisco Unified CallManager cluster because this arrangement allows each account to be granted specific permissions only when needed and allows for easier administration on a per-cluster basis without the risk of affecting other parts of the enterprise. In the examples in this chapter, this account is called the CCM Directory Manager, but the name you choose for this user account may be different.

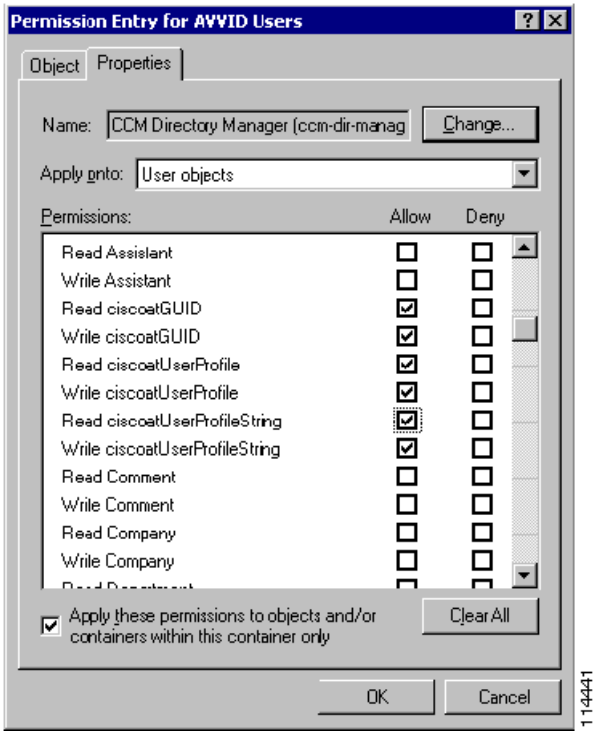
Each CCM Directory Manager account should be granted at least the following permissions within your directory:

- **Read/Write/Create all child objects/Delete all child objects** privileges on the respective "Cisco" OU subtrees. The rights must be set to apply to **This object and all child objects** for both the object and the properties. In AD, you can set this privilege by using the advanced options for security within Active Directory Users and Computers (ADUC). The default is to apply to the object only, so you will have to change the rights.

- **Read** privileges on all the OUs contained at and below the User Search Base. You can set this privilege just at the User Search Base level, as long as inheritance is not blocked lower in the tree.
- **Read/Write** privileges on the ciscoatGUID, ciscoatUserProfile, and ciscoatUserProfileString attributes for all User objects contained below the User Search Base. In AD, you can set this privilege by using the advanced options for security within ADUC.

Tip In AD, to set the permissions for the ciscoatGUID, ciscoatUserProfile, and ciscoatUserProfileString attributes for all User objects within the User Search Base, select the CCM Directory Manager user from the Advanced security window for the organizational unit (OU) at the root of the User Search Base. (In this chapter, the user is called CCM Directory Manager, but your user name may be different.) Then click **View/Edit** and go to the **Properties** tab of the new window, as shown in Figure 18-8. From the **Apply onto** drop-down menu, select **User objects**, and then scroll down to the ciscoatGUID, ciscoatUserProfile, and ciscoatProfileString attributes. Allow **Write** permissions for all of them.

Figure 18-8 Setting Permissions for the User Account in Active Directory



Tip While creating the CCM Directory Manager account, set the **Password never expires** option. When you want to change the password, run the CCMPwdChanger utility from Cisco Unified CallManager. This method updates the password in AD, updates the registry in Cisco Unified CallManager, and updates directory initialization files.

Integrating Cisco Unified CallManager with the Directory

After you have prepared the directory as described in the preceding section, you can perform the integration by running the Cisco Customer Directory Configuration plugin again. The two key concepts to consider at this point are the User Search Base and the User Creation Base.

Note The User Creation Base was introduced in Cisco Unified CallManager Release 4.0. In previous versions of Cisco Unified CallManager, the User Search Base is also used for user creation.

As mentioned in the preceding section, the User Search Base parameter represents the root of the subtree used by Cisco Unified CallManager for all user searches.

The User Creation Base parameter tells Cisco Unified CallManager where to create the following system accounts, which are needed by some applications and the features bundled with them:

- CCM Administrator, used by Cisco Unified CallManager Multilevel Administration Access (MLA)
- CCM SysUser, used by CallBack and Extension Mobility
- IPMA SysUser, used by Cisco IP Manager Assistant

The User Creation Base must be contained within the User Search Base because Cisco Unified CallManager has to be able to search for the system account users before authenticating them.

To set the User Search Base, look at where the users serviced by the cluster are located, and set the User Search Base to the first level that includes all of them. The lower you set the User Search Base, the better response times and performance you achieve because searches will not have to follow many referrals and cross slow WAN links to get to remote domain controllers. Also, user data not needed by the cluster does not have to be parsed in the search.

In a single-domain AD forest (or standalone Netscape Directory), set the User Search Base to the lowest organizational unit (OU) that contains all potential users for the Cisco Unified CallManager cluster (for example: ou=AVVID Users, dc=vse, dc=lab). This OU might even be the root of the domain (for example: dc=vse, dc=lab, or o=avvid.lab) if users are spread across a set of OUs directly under this one.

In a multiple-domain AD forest, try to keep the users for a specific Cisco Unified CallManager cluster within a single domain, and follow the guidelines described previously. If a single domain is not possible because users are spread across multiple domains, set the User Search Base to the lowest point in the tree containing all domains with users serviced by the Cisco Unified CallManager cluster. In structures in which serviced child domains are under the top-level domain, the User Search Base must be set at the root of the entire AD forest. In all cases, though, try to ensure that a domain controller for each serviced domain is collocated with Cisco Unified CallManager, or that the network is sufficiently resilient and fast to allow remote searches with no greater performance degradation than occurs with local searches.

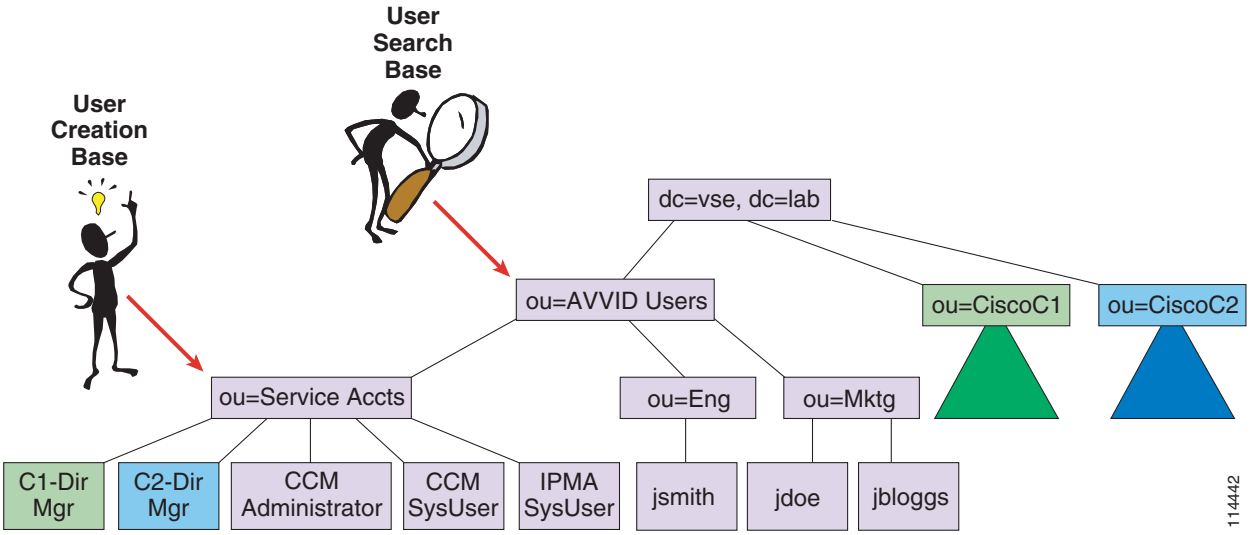
Note Although the User Creation Base must exist within the User Search Base, take care to ensure that no existing Active Directory user policies are applied to the system accounts created there. A simple way to protect the system accounts from user policies is to put the accounts in a sub-OU and block inheritance of the Group Policy Object (GPO) to that OU.

It is possible to integrate multiple Cisco Unified CallManager clusters with the same AD forest. However, due to the potentially large number of 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 request specific support from the Cisco engineering team before proceeding with a multi-cluster integration. Contact your local Cisco account representative to initiate the support request. When deploying Cisco voice applications other than Cisco Unified CallManager (such as the CDR

Analysis and Reporting tool, Multilevel Administration Access, Unified Contact Center Enterprise, Unified Contact Center Express, and so forth), additional limitations may apply. Refer to the respective online documentation and release notes for details on these other products

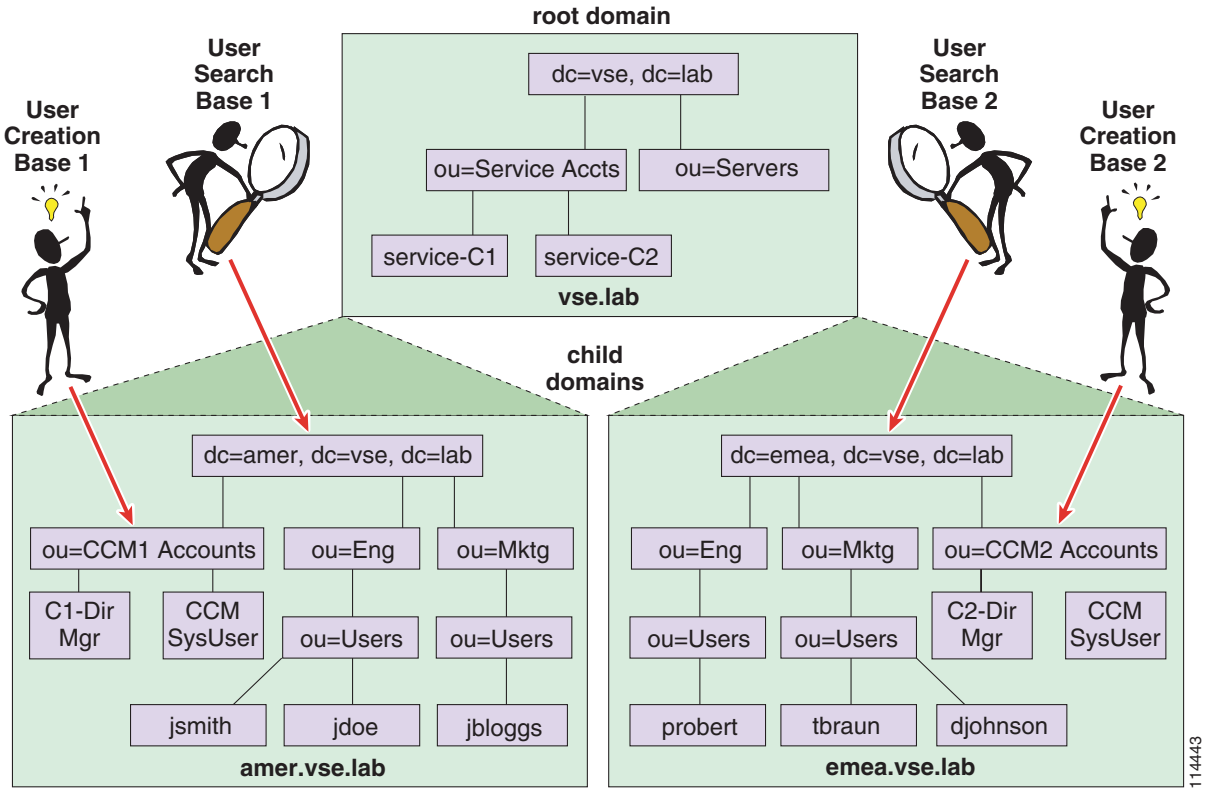
When integrating multiple Cisco Unified CallManager clusters with the same AD domain (or standalone Netscape Directory), you can share the system accounts across clusters by specifying the same User Creation Base, as shown in Figure 18-9.

Figure 18-9 Setting the User Search Base and User Creation Base in a Single AD Domain



When integrating multiple Cisco Unified CallManager clusters with different AD domains within a forest, Cisco recommends that you define a different User Creation Base for each cluster, setting it to an OU within the relevant domain, as shown in Figure 18-10.

Figure 18-10 Setting the User Search Base and User Creation Base in a Multiple-Cluster, Multiple-Domain Forest



Tip You can prevent system and service accounts from appearing in Cisco Unified CallManager Administration by adding the string **CiscoPrivateUser** to the user's Description field. The CCM Administrator, CCM SysUser, and IPMA SysUser accounts have this field set by default, but you can safely add the description to the CCM Directory Manager account as well. Use Microsoft ADSIEdit (Active Directory Service Interfaces, available as a part of the Windows 2000 Support Tools) or any other LDAP tool to update the Description field.

After you have decided how to set the User Search Base and User Creation Base, you can run the Cisco Customer Directory Configuration plugin again on the Cisco Unified CallManager publisher server within your cluster. Follow these best practices when performing this step:

- Select the **Custom** plugin setup type, and select the **Configure Active Directory** and the **Enable CallManager Integration with Active Directory** options only.
- Specify the host name of a domain controller located within the same LAN as Cisco Unified CallManager, or use the domain name if you are using DNS and all domain controllers for this domain are located in the same LAN as Cisco Unified CallManager. Refer to Planning the Directory Integration, page 18-13, for more details on how to provide high availability for the directory integration.

After completing these steps on the publisher server, set the passwords for the three system accounts by using either the CCMPwdChanger tool bundled with Cisco Unified CallManager (open a DOS window by selecting **Start** > **Run**, type **cmd**, enter **CCMPwdChanger**, and press **Enter**) or your corporate

directory's interface (for example, ADUC in the case of Active Directory). Cisco recommends that you set the password policy for these users so that their passwords never expire and are not set to change on first logon. This password policy is also one reason to avoid having any GPOs applied to these accounts.

If you enforce an expiration policy, Cisco Unified CallManager will stop working when the password expires, and there will be no warning to alert you that the problem is an expired password. If you have policies that require password changes every three months, for example, you should run the CCMPwdChanger tool every three months.

After completing all the preceding steps, you can run the Cisco Customer Directory Configuration plugin on every subscriber server within the Cisco Unified CallManager cluster.

Note When you perform the integration, no data migration occurs between the Cisco Unified CallManager embedded directory and the corporate directory. If you want to migrate users and profiles that you had configured in the embedded directory, Cisco has developed some migration scripts that can help you in this task. To obtain these scripts, contact your Cisco account team or channel partner. Note that the scripts are provided as-is and without support.

Maintaining the Directory Integration

After you have integrated Cisco Unified CallManager with an external directory, you should set the user and password management procedures and policies accordingly.

Use the corporate directory's interface (or supported API) for the following administrative operations:

- Adding a user
- Removing a user
- Setting and changing the core user attributes (such as display name, department, address, and password)

In addition, use Cisco Unified CallManager Administration for the following administrative operations:

- Configuring CallManager-specific user attributes (such as PIN and user locale)
- Associating a user with a device (such as an IP phone or a CTI port)

By default, you cannot use Cisco Unified CallManager Administration to add or remove users. You also cannot modify any of their core user attributes, such as name and phone number. If you want to enable adding and removing users in Cisco Unified CallManager Administration, you can modify the UMDirectoryConfiguration.ini file on the Cisco Unified CallManager servers, as described in *Installing the Cisco Customer Directory Configuration Plugin for Cisco CallManager Release 4.0(1)*, available at

http://www.cisco.com

This functionality, 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.

Even if Cisco Unified CallManager is integrated with Microsoft Active Directory, you still cannot set or modify user passwords through Cisco Unified CallManager Administration because Active Directory does not allow passwords to be set through clear-text LDAP. To change directory passwords in a secure fashion, you can use either the CCMPwdChanger tool bundled with Cisco Unified CallManager or the management interface provided by the directory vendor.

Even after modifying the UMDirectoryConfiguration.ini file on Cisco Unified CallManager, you still have to give the CCM Directory Manager account sufficient permissions to create and delete users in AD.

When integrating multiple Cisco Unified CallManager clusters with the same directory, keep in mind that you cannot associate the same user with devices in different clusters. Each user must be associated with a single, specific Cisco Unified CallManager cluster at any point in time. (You can, of course, move users from one cluster to another by simply disassociating them from devices in the first cluster and associating them to devices in the second cluster.)

For user-initiated password changes and the setting of preferences, instruct your users to do the following:

- Use the directory application's interface to change their passwords. In the case of Microsoft Active Directory, password changes are done through the users' Windows workstations or by the administrator using the management tools.
- Use the Cisco Unified CallManager User Options web page to change PINs and Cisco Unified CallManager preferences (such as speed dials and call-forward-all numbers).

Note Although the Cisco Unified CallManager User Options web page allows users to change their passwords even after integration with AD, Cisco does not recommend this practice because users probably will not realize that they are changing their Windows passwords at the same time. Also, the communication between the client workstation and the Cisco Unified CallManager server uses HTTP, so the password would travel across the network in clear text. You can remove the **Change your Password** option from the Cisco Unified CallManager User Options web page simply by removing the relevant code from the active server page (ASP).

As far as adds, moves, and changes are concerned, be aware that the following operations are not supported when Cisco Unified CallManager is integrated with the directory:

- Changing a username (in the case of AD, this is the sAMAccountName)
- Moving a user from one OU to another
- Moving or renaming the "Cisco" OU

However, to work around these restrictions, you can manually delete the user's CallManager-specific attributes (such as the profile in the "Cisco" OU and the data in the ciscoatGUID, ciscoatUserProfile, and ciscoatUserProfileString attributes for the user in question). Then the user can be renamed or moved using the directory management tools before being re-added as a Cisco Unified CallManager subscriber. Although it is more cumbersome, this procedure preserves the user’s file ownership and security principles in the directory application.

Cisco Unified CallManager Upgrades

Because the schema might change with every major Cisco Unified CallManager release, you should run the Cisco Customer Directory Integration plugin after every upgrade.

If you have integrated multiple Cisco Unified CallManager clusters with the same directory, you need to extend the schema only once. If the clusters are running different Cisco Unified CallManager releases, you should extend the schema from within the cluster that is running the most recent release.