How to Configure Unified Communications Manager Directory Integration in a Multi-Forest Environment

Contents

Introduction **Prerequisites** Requirements **Components Used** Preface **Overview** Active Directory Multiple Forest Support Scenario in CUCM **Domain Trust Relationship Install AD LDS** Install AD LDS in 2008 Install AD LDS in 2012 Install the Instance for Multiple Forest Support Multiple Forest Support in 2008 Multiple Forest Support in 2012 **Configure ADAM Schema Analyzer** Extend the AD LDS Schema with the User-Proxy Objects Import the Users From AD DC to AD LDS Create the User in AD LDS for CUCM Synchronization and Authentication **Configure Bind Redirection Configure CUCM** LDAP Filters in CUCM

Introduction

This document discusses how to configure Cisco Unified Communication Manager (CUCM) Directory Integration in a Multi-Forest Environment.

Prerequisites

Requirements

Cisco recommends that you have:

- 1. Knowledge of deployment and configuration of CUCM directory integration.
- Knowledge of deployment and configuration of Microsoft Active Directory Application Manager (ADAM) 2003 or Microsoft Lightweight Directory Services (AD LDS) 2008 or 2012.
- 3. CUCM Release 9.1(2) or later.

- 4. When you use CUCM Release 9.1(2) or later, the LDAP filter can be changed with the Administrative web interface.
- 5. The number of user accounts to be synchronized must not exceed 60,000 accounts per CUCM Publisher. When more than 60,000 accounts need to be synchronized, the IP Phone Services Software Development Kit (SDK) must be used in order to provide a custom directory. See the <u>Cisco Developer Network</u> for additional details. When you use Unified CM Release 10.0(1) or later, the maximum number of user accounts supported is 160,000.
- 6. Microsoft ADAM 2003 or Lightweight Directory Services (LDS) 2008 or 2012.
- 7. The requirement for SSL when you use bind redirection should not be disabled. If it is disabled, it causes the password of a Windows security principal to pass to the computer that runs ADAM without encryption. Thus, it should be disabled only in a test environment.
- 8. User ID (sAMAccountName) needs to be unique across all the forests.
- 9. If there is an AD LDS setup and if the CUCM UserID mapped to sAMAccountName needs to be used, then that agreement should be configured as the AD.
- 10. When you configure the domain trust relationship between ADAM instance host domain and user accounts host domain, the domain functional level and the forest functional level should be 2003 or later.
- 11. CUCM supports only a single application directory partition in AD LDS, multi partition is not supported currently.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Preface

Microsoft AD LDS, formerly known as ADAM, can be used to provide directory services for directory-enabled applications. Instead of using your organization's Active Directory Domain Service (AD DS) database in order to store the directory-enabled application data, AD LDS can be used to store the data. AD LDS can be used in conjunction with AD DS so that you can have a central location for security accounts (AD DS) and another location in order to support the application configuration and directory data (AD LDS). With AD LDS, you can reduce the overhead associated with AD replication, you do not have to extend the AD schema in order to support the application, and you can partition the directory structure so that the AD LDS service is only deployed to the servers that need to support the directory-enabled application.

- Install from Media Generation The ability to create installation media for AD LDS with Ntdsutil.exe or Dsdbutil.exe.
- Audit Audit changed values within the directory service.
- Database Mounting Tool Gives you the ability to view data within snapshots of the database files.
- AD Sites and Services Support Gives you the ability to use AD Sites and Services in order to manage the replication of the AD LDS data changes.
- Dynamic List of LDIF files With this feature, you can associate custom LDIF files with the

current default LDIF files used for setup of AD LDS on a server.

• Recursive Linked-Attribute Queries - LDAP queries can follow nested attribute links in order to determine additional attribute properties, such as group memberships.

There are a lot of differences between ADAM and AD, ADAM can only deliver part of the functions delivered by AD.



Overview

The objective of this document is to explain the mechanisms that allow CUCM, or any other Cisco products that use Directory Integration Service (DirSync), to get user information and perform authentication from different AD domains that can exist in different forests. In order to achieve this objective, ADAM is used in order to synchronize its user database with different AD Domain Controllers or other LDAP sources.

ADAM can create a database of users and store their details. Single Sign On (SSO) functionality is desired in order to avoid end users having to maintain different sets of credentials in different systems; therefore, ADAM bind redirection is used. ADAM bind redirection is a special function for applications that support LDAP bind as an authentication mechanism. In some cases, the special schema, or naming context, might force you to avoid AD, which makes ADAM a necessary choice. This avoids users having to remember multiple passwords due to the employment of an additional directory with its own user ID and password.

A special user proxy object in ADAM maps to a regular AD user account. The user proxy does not have an actual password stored in the ADAM object itself. When the application performs its normal bind operation, it checks the ID locally, but checks the password against AD under the covers as shown in this figure. The application does not need to be aware of this AD interaction.



ADAM bind redirection should be used only in special cases where an application can perform a simple LDAP bind to ADAM. However, the application still needs to associate the user with a security principal in AD.

ADAM bind redirection occurs when a bind to ADAM is attempted with use of a special object called a proxy object. A proxy object is an object in ADAM that represents a security principal in AD. Each proxy object in ADAM contains the SID of a user in AD. When a user attempts to bind to a proxy object, ADAM takes the SID that is stored in the proxy object, together with the password that is supplied at bind time, and presents the SID and the password to AD for authentication. A proxy object in ADAM does not store a password, and users cannot change their AD passwords through ADAM proxy objects.

The password is presented in plain text to ADAM because the initial bind request is a simple LDAP bind request. For this reason, an SSL connection is required by default between the directory client and ADAM. ADAM uses Windows Security APIs in order to present the password to AD.

You can get more information on bind redirection in Understanding ADAM bind redirection .

Active Directory Multiple Forest Support Scenario in CUCM

In order to explain the method, imagine a scenario where Cisco Systems (Forest 2) has acquired two other companies: Tandberg (Forest 3) and Webex (Forest 1). In the migration phase, integrate the AD structure of each company in order to allow the deployment of a single Cisco Unified Communications cluster.



In the example, company Cisco (Forest 2) has two domains, Forest root domain called CISCO (dns cisco.com) and a subdomain called EMERG (dns emerg.cisco.com). Both of these domains have a Domain Controller that is also a Global Catalog, and each one is hosted in Windows 2008 Server SP2.

Company Tandberg (Forest 3) has a single domain with a Domain Controller that is also a Global Catalog, and it is hosted in Windows 2008 Server SP2.

Company Webex (Forest 1) has a single domain with a Domain Controller that is also a Global Catalog, and it is hosted in Windows 2003 R2 Server SP2.

AD LDS is installed in the Domain Controller for domain CISCO, or can be a separate machine; in fact it could be anywhere in one of the three forests. The DNS infrastructure must be in place such that domains in one forest can communicate with domains in other forests and to establish the appropriate trust relationships and validations between the forests.

Domain Trust Relationship

For the authentication of the users to work, you need to have a trust between the domain where the ADAM instance is hosted, and the other domain(s) that hosts the user accounts. This trust can be a one-way trust if required (outgoing trust from the domain that hosts the ADAM instance to the domain(s) that hosts the user accounts). This way, the ADAM instance will be able to forward the authentication requests to DCs in those account domains.

Furthermore, you will need to have a user account from both account domains that has access to all attributes of all user accounts in the domain. This account is used by ADAMSync in order to synchronize the Account Domain users to ADAM.

Last but not least, the machine that runs ADAM must be able to find all domains (DNS), find domain controllers in both domains (with DNS), and connect to these Domain Controllers.

Complete these steps in order to set up the intertrust relationships:

1. Open Active Directory Domains and Trusts, right-click the domain that hosts AD LDS, and choose **Properties**.



2. Click the Trusts tab, and click New Trust.

Relative Directory Domains and True	ts	
File Action View Help		
🗢 🧼 🖄 📰 📄 📓 🖬		
Active Directory Domains and Trusts [a	cisco.com Properties	Actions
emerg.cisco.com	General Trists Mananed By	cisco.com 🔺
	Domains trusted by this domain (a doning trusts):	More Actions
	Domain Name Trust Type Transitive Properties	
	emerg.cisco.com Child Yes Remove	
	Domains that to st this domain (nonming to ste):	
	Domain Name Trust Type Transtive Properties	
	emerg.cisco.com Child Yes Remove	
	Nev Trust	
	OV Creat Costs Hith	
	Cance Adday Hep	
	,	

3. Follow the wizard and enter the name of the domain that you want to establish the trust with. Click **Next**.

New Trust Wizard			×
Trust Name You can create a trust by using a NetBIOS or	DNS name.		
Type the name of the domain, forest, or realm for th must type a DNS name.	iis trust. If you	type the name of	a forest, you
Example NetBIOS name: supplier01-int Example DNS name: supplier01-internal.microsoft.c	:om		
N <u>a</u> me:			
tandberg			
N			
kz			
	< <u>B</u> ack	<u>N</u> ext >	Cancel
-			

4. Click the Forest trust radio button. Click Next.

New Trust Wizard	×
Trust Type This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.	
Select the type of trust you want to create.	
External trust An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.	
Forest trust A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.	
R	
< <u>B</u> ack <u>N</u> ext > Cancel	

5. On the direction of the trust only 'one-way: outgoing' is required. Click the **One-way: outgoing** radio button. Click **Next**.

cisco.com	Properties	? ×		Actions
General	Trusts Managed By			cisco.com
Domain	s trusted by this domain (outgoing trusts):	1		More Actic
New	Trust Wizard			×
	Direction of Trust You can create one-way or two-way trusts.			
	Select the direction for this trust.			
	Two-way Users in this domain can be authenticated in the specific forest, and users in the specified domain, realm, or fore this domain.	ified domain, est can be au	, realm, or uthenticat	ed in
-	One-way: incoming Users in this domain can be authenticated in the spec	ified domain,	, realm, or	forest.
	One-way: outgoing Users in the specified domain, realm, or forest can be	authenticate	d in this d	omain.
_				
	< Back	Next	>	Cancel

6. Allow the wizard to configure both domains. Click the **Both this domain and the specified domain** radio button. Click **Next**.

cisco	o.com Properties	? ×		Actions
Ge	eneral Trusts Managed By			cisco.com
D)omains trusted by this domain (outgoing trusts):	1		More Action
	New Trust Wizard			×
	Sides of Trust If you have appropriate permissions in both domains, you ca the trust relationship.	in create b	ooth sides	of
	To begin using a trust, both sides of the trust relationship mu if you create a one-way incoming trust in the local domain, a must also be created in the specified domain before authent flowing across the trust.	ist be crea one-way ication tra	ited. For ex outgoing ti ffic will beg	xample, rust gin
Г	Create the trust for the following:			
	C This domain only This option creates the trust relationship in the local dom	iain.		
	 Both this domain and the specified domain This option creates trust relationships in both the local an You must have trust creation privileges in the specified of 	nd the spe Iomain.	cified dom	iains.
	< Back	Next	>	Cancel

7. Enter the credentials for the other domain. Click Next.

cisco	o.com Properties		?×	Actions
Ge	eneral Trusts Managed By			cisco.com
	Domains trusted by this domain (outgoing trusts):			More Actio
	New Trust Wizard			×
-	User Name and Password To create this trust relationship, you mus domain.	st supply user credent	ials for the specifi	ed 🧖
	Specified domain: tandberg			
	Type the user name and password of ar	n account in the spec	ified domain.	
F	User name: 🙍 tandberg 🖓	Iministrator		•
	Password:			
		< Back	Next >	Cancel

8. Click the Forest-wide authentication radio button. Click Next.

cisco	o.com	n Properties				? ×	Actions
Ge	neral	Trusts Man	aged By				cisco.com
D	omair	ns trusted by this	domain (out	aoina trusts):			Piore Acto
	New	Trust Wizard					×
-	(Dutgoing True Users in the local forest	st Authentic specified for or only those	cation Level- est can be auth resources that y	Local Forest enticated to use all o rou specify.	of the resources	in the
		Select the s	cope of auth	entication for us	ers from the tandberg	g forest.	
Ē		 Forest-w Window in the lo organiza 	ide authentic s will automa cal forest. Th tion.	ation tically authentic: is option is prefe	ate users from the sp med when both fore:	pecified forest fo sts belong to the	r all resources e same
		C Selectiv Window resource domain option is	e authenticat s will not auto s in the local and server th preferred if t	tion omatically authe I forest. After you at you want to n he forests belon	nticate users from th u finish this wizard, g nake available to use g to different organiz	e specified fore: rant individual a ers in the specifi ations.	st for any ccess to each ed forest. This
					< Back	Next >	Cancel

9. Click the Yes, confirm the outgoing trust radio button. Click Next.

New Trust Wizard			X
Confirm Outgoing Trust You should confirm this trust only if the oth	her side of the trust h	nas been created	. 🤗
Do you want to confirm the outgoing trust	?		
O No, do not confirm the outgoing trust			
 Yes, confirm the outgoing trust 			
	R		
To confirm the trust now, click Next.			
	< Back	Next >	Cancel

This is the result that you receive after you run this process for both the Tandberg and Webex domains. The domain emerg is there by default since it is a child domain. Click **OK**.

cisco.com Properties			? ×
General Trusts Managed B	3y]		
Domains trusted by this doma	ain (outgoing tr	usts):	
Domain Name emerg.cisco.com tandberg.com webex.com	Trust Type Child Forest Forest	Transitive Yes Yes Yes	Properties Remove
Domains that trust this domain	n (incom o tru Trust Type	sts): Transitive	Properties
emerg.cisco.com	Child	res	Remove
New Trust			
ОК	Cancel	Apply	Help

Install AD LDS

Install AD LDS in 2008

1. Open Server Manager, click Roles, and click Add Roles.



2. Check the Active Directory Lightweight Directory Services check box. Click Next

Next. Add Roles Wizard		X
Select Server Roles	;	
Before You Begin Server Roles AD LDS Confirmation Progress Results	Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Pederation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Directory Server Directory Server Directory Rights Management Services Directory Server Directory Server Directory Rights Management Services Directory Server Dire	> Install Cancel X

3. The AD LDS Services Installation Progress window appears. Add Roles Wizard

Installation Progr	ess
Before You Begin Server Roles AD LDS Confirmation Progress Results	The following roles, role services, or features are being installed:
	Initializing installation <previous next=""> Install Cancel</previous>

Install AD LDS in 2012

Complete these steps in order to set up AD LDS in 2012:

1. Open Server Manager and choose Add Roles and Features. Click Next and click Installation Type in order to move to the Installation Type page.



- Configure a single server by adding roles, role services, and features.
- Remote Desktop Services installation

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

- < Previous Install Cancel
- 3. Click the **Select a server from the server pool** radio button in order to select the default server. Click **Next**.

à	Add Role	s and Features	Wizard 📃 🗖 🗙			
Select destinati	on server		DESTINATION SERVER WIN-IGS93VLG8M4.childExperiment.citg2012r2.india.com			
Before You Begin Installation Type Server Selection	Select a server or a virtual Select a server from the Select a virtual hard dis	 Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk 				
Server Roles Features Confirmation Results	Server Pool Filter: Name WIN-IGS93VLG8M4.chil 1 Computer(s) found This page shows servers th Add Servers command in S collection is still incomplet	IP Address 10.77.29.55 nat are running Wi Server Manager. O te are not shown.	Operating System Microsoft Windows Server 2012 R2 Standard			
		< <u>P</u> r	evious Next > Install Cancel			

4. Check the Active Directory Lightweight Directory Services check box and click Add Features. Continue with the installation.

à	Add Roles	and Features Wizard
Select server roles Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles Select one or more roles to Roles Active Directory C Active Directory C Active Directory D Active Directory Fe Active Directory Fi Active Directory Ri Active Directory Ri DHCP Server DNS Server (Install	Add features that are required for Active Directory Lightweight Directory Services? The following tools are required to manage this feature, but do not have to be installed on the same server. A Remote Server Administration Tools A D DS and AD LDS Tools [Tools] AD LDS Snap-Ins and Command-Line Tools
	 Fax Server File and Storage Server Hyper-V Network Policy an Print and Docume Remote Access Remote Desktop Server 	[Tools] AD LDS Snap-Ins and Command-Line Tools

- 5. Click **Next** in the subsequent pages.
- 6. Click the Restart the destination server automatically if required checkbox and click

Install in order to install the feature.



Install the Instance for Multiple Forest Support

AD LDS can run different instances of the services with different ports which allows for different user directory "applications" to be run on the same machine. By default AD LDS chooses ports 389/LDAP and 636/LDAPS, but if the system already has any kind of LDAP services that run them it will use ports 50000/LDAP and 50001/LDAPS. Each instance will have a pair of ports that increment based on the previous numbers used.

In some cases, due to a Microsoft bug, the ports are already used by the Microsoft DNS server and the instance wizard gives an error (which is not self-explanatory). This error can be fixed when you reserve the ports in the TCP/IP stack. If you find this problem, see <u>AD LDS service start fails</u> with error "setup could not start the service..." + error code 8007041d.

Multiple Forest Support in 2008

1. In the server manager, choose **Roles** and then **Active Directory Lightweight Directory Services**. Click **Click here to create an AD LDS instance**.

Server Hanager					
File Action View Help					
he 🔿 🔁 📅 🔢					
Server Manager (AD2K8-1)	Active Directory Lightweight Directory Services				
Poes Active Directory Domain Se Active Directory Lightweigh E DNS Server Fastures Degnostics	Provides a store for application-specific directory data.				
	Summary				
 Configuration Storage 	No AD LOS instances have been created. Click here to create an AD LOS instance.				
	Events: None in the last 24 hours	g Go to Event Viewer			
	Pause Pause	Fiter Events			
		Properties			
	La La				
	Advanced Tools				
	Create a new AD LDS instance	AD LDS Setup Wizard			
	Query, view, and edit objects and attributes in the directory	DSI Edit			
	Perform LDAP operations against the directory such as connect, bind, search, modify, add, and delete	🖬 Láp.exe			
	Resources and Support				
1	Recommended configurations, tasks, best practices, and online resources	AD LDS Help			
	I Vir Less Nomesh: sul/zs/zula 6(4/) 49 PM Configure remesh				

2. Click the A unique instance radio button. Click Next.

Active Directory Lightweight Directory Services Setup Wizard
Setup Options An AD LDS instance is created each time AD LDS is installed.
You can create a unique instance, or you can install a replica of an existing instance.
Select the type of instance you want to install.
A unique instance
This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.
A replica of an existing instance
This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.
< Back Next > Cancel Help

3. In the Instance name field, enter the name of the instance. It is MultiForest in this example. Click **Next**.

Instance Name The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.	
Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.	
Instance name: MultiForest	
Example: Addressbook 1	
The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services.	
AD LDS service display name: MultiForest AD LDS service name: ADAM_MultiForest	
< Back Next > Cancel Hel	p

X

4. Enter the selected LDAP port number and SSL port number or allow the system to choose them for you. Click **Next**.

	Active Directory Lightweight Directory Convises Coture Wissard
20	Active Directory Lightweight Directory Services Setup wizard

Ports Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.
The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.
If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.
LDAP port number:
SSL port number: 50001
< Back Next _N > Cancel Help

5. **Note**: CUCM supports only single application directory partition, multi partition is not supported currently.

See <u>Step 5: Practice Working with Application Directory Partitions</u> for information on how to create an Application Directory Partition. The process to create a directory partition for each domain that you want to synchronize against works based on LDAP referral (RFC 2251) and requires that the LDAP client (CUCM, CUP, and so on) supports referrals.Click the **Yes**, **create an application directory partition** radio button. Enter the partition name in the Partition name field for the instance. Do not provide a cn like in the example of the wizard, because most of the time that creates an error in the Schemas. In this scenario, the same partition as the AD domain controller that hosts AD LDS (dc=Cisco,dc=com) was entered. Click **Next**.

Nζ

х

Active Directory Lightweight Directory Services Setup Wizard					
Application Directory Partition An application directory partition stores application-specific data.					
Do you want to create an application directory partition for this instance of AD LDS?					
O No, do not create an application directory partition					
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.					
Yes, create an application directory partition					
Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name: CN=Partition1,DC=Woodgrove,DC=COM					
Partition name:					
DC=cisco,DC=com					
< Back Next > Cancel Help					

6. Click the **This account** radio button. Enter a User name and Password in order to start the server. Click **Next**.

Active Directory Lightweight Directory Services Setup Wizard
Service Account Selection AD LDS performs operations using the permissions associated with the account you select.
Set up AD LDS to perform operations using the permissions associated with the following account.
Network service account
AD LDS has the permissions of the default Windows service account.
 This account: AD LDS service has the permissions of the selected account.
User name: 🖸 CISCO\Administrator 🔽 Browse
Password:
< Back Next > Cancel Help

 Click the Currently logged on user radio button. Enter the name of the user with administrative permissions. Click Next.

Active Directory Lightweight Directory Services Setup Wizard	×
AD LDS Administrators You can specify the user or group that will have administrative privileges for this instance of AD LDS.	
Assign the following user or group of users administrative permissions for AD LDS.	
Currently logged on user: CISCO\Administrator The user that is installing AD LDS will have administrative permissions for this instance of AD LDS.	
C This account The selected user or group will have administrative permissions for this instance of AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.	vf
Account name: Browse	
< Back Next > Cancel	Help

8. Import the highlighted default LDIF files in order to build the schema. Click Next.

Importing LDIF Files

You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.

LDIF file name	Description			
MS-AdamSyncMetadata.LDF	ADAMSync metadata schema extension. Required for A			
MS-ADLDS-DisplaySpecifiers	AD LDS Display specifiers schema and display specifier			
MS-AZMan.LDF	AD LDS schema extensions for AzMan.			
 MS-InetOrgPerson.LDF 	AD LDS inetOrgPerson, user and related classes.			
MS-User.LDF	AD LDS user class and related classes.			
MS-UserProxy.LDF	AD LDS simple userProxy class.			
MS-UserProxyFull.LDF	AD LDS full userProxy class. Requires MS-User.LDF or			
•	•			

Note: If ADAM is installed on a Windows 2003 sever, then the previous screen will have only four options: MS-AZMan.LDF, MS-InetOrgPerson.LDF, MS-User.LDF, and MS-UserProxy.LDF. From these four, check only the check boxes for MS-User.LDF and MS-InetOrgPerson.LDF.

Multiple Forest Support in 2012

1. Open the Administrative tools and double-click Active Directory Lightweight Directory Services Setup Wizard.

X

🕲 I ⊋ 🔝 = I		Shortcut Tools	Application Tools	Administrat	ive Tools		x	
File Home Share	View	Manage	Manage				~ ()
🍥 💿 🔻 † 🔞 « System and Security 🕨 Administrative Tools 🛛 🗸 🖒				Search Administration	ve Tools	٩		
	Name		*		Date modified	Type		
💢 Favorites					b dec mouned	(Jps	-	1
Desktop	퉬 Termi	nal Services			8/22/2013 8:39 AM	File folder		
Downloads	🛐 Active	Directory Admir	nistrative Center		8/21/2013 4:50 PM	Shortcut		
📃 Recent places	📸 Active	e Directory Doma	ins and Trusts		8/21/2013 11:55 PM	Shortcut	_	
	🖪 Active	Directory Lightw	veight Directory Serv	vices Setup Wizard	8/21/2013 11:56 PM	Shortcut		
p This PC	🔊 Active	Directory Modu	le for Windows Pow	erShell	8/21/2013 11:55 PM	Shortcut		
0	Active 🚽	Directory Sites a	ind Services		8/21/2013 11:55 PM	Shortcut		
👊 Network	🖹 Active	Directory Users	and Computers		8/21/2013 11:55 PM	Shortcut	=	i
	😿 ADSH	Edit			8/21/2013 11:55 PM	Shortcut		
	📷 Certifi	ication Authority			8/21/2013 11:56 PM	Shortcut		
	🔊 Comp	onent Services			8/21/2013 11:57 PM	Shortcut		
	💦 Comp	uter Manageme	nt		8/21/2013 11:54 PM	Shortcut		
	🛅 Defrag	gment and Optin	nize Drives		8/21/2013 11:47 PM	Shortcut		
	💰 DNS				8/21/2013 11:55 PM	Shortcut		
	😹 Event	Viewer			8/21/2013 11:55 PM	Shortcut		1
	😹 Group	Policy Manager	nent		8/21/2013 11:56 PM	Shortcut		
	騇 Intern	et Information Se	ervices (IIS) Manager	r	8/21/2013 11:50 PM	Shortcut		
	🙈 isosi i	Initiator			8/21/2013 11:57 PM	Shortcut		
	🗟 Local	Security Policy			8/21/2013 11:54 PM	Shortcut		
	📷 ODBC	Data Sources (3)	2-bit)		8/21/2013 4:56 PM	Shortcut		
	🛐 ODBC	Data Sources (64	4-bit)		8/21/2013 11:59 PM	Shortcut		
	💱 Onlin	e Responder Mar	agement		8/21/2013 11:56 PM	Shortcut		
	🛞 Perfor	mance Monitor			8/21/2013 11:52 PM	Shortcut	~	,
	<		Ш				>	1
35 items 1 item selected	1.13 KB					995	=	

2. Click Next.



3. Check the A unique instance radio button. Click Next.

Active Directory Lightweight Directory Services Setup Wizard			
Setup Options An AD LDS instance is created each time AD LDS is installed.			
You can create a unique instance, or you can install a replica of an existing instance.			
Select the type of instance you want to install.			
This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.			
A replica of an existing instance			
This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.			
< <u>B</u> ack <u>N</u> ext > Cancel Help			

4. Enter an Instance Name and Description for the instance. The name "MultiForest" is entered here. Click **Next**.

	Active Directory Lightweight Directory Services Setup Wizard		
In	stance Name The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.		
	Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.		
	Instance name:		
	MultiForest		
	Example: Addressbook1		
	Description:		
	AD LDS instance		
The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter. AD LDS service display name: MultiForest AD LDS service name: ADAM_MultiForest			
	< <u>B</u> ack <u>N</u> ext > Cancel Help		

5. Enter the LDAP and SSL port numbers. The preferred ports are 389 and 636 respectively. If the domain server is a child server and if the parent domain uses these ports, then by default different port numbers will be populated. In that case, do not change them and continue with the installation. Click **Next**.

	Active Directory Lightweight Directory Services Setup Wizard			
Po	rts Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.			
	The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below. If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.			
	LDAP port number: 389 SSL port number: 636			
	< <u>B</u> ack <u>N</u> ext > Cancel Help			

6. Here, by default, other port numbers have been populated. Click Next.

	Active Directory Lightweight Directory Services Setup Wizard		
Po	orts Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.		
The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below. If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.			
	LDAP port number: 50000 SSL port number: 50001		
	< <u>B</u> ack <u>N</u> ext > Cancel Help		

7. **Note**: CUCM supports only single application directory partition, multi partition is not supported currently.

See <u>Step 5: Practice Working with Application Directory Partitions</u> for information on how to create an Application Directory Partition. The process to create a directory partition for each domain that you want to synchronize against works based on LDAP referral (RFC 2251) and requires that the LDAP client (CUCM, CUP, and so on) supports referrals. See <u>Microsoft</u> <u>Support</u> for more information.Click the **Yes, create an application directory partition** radio button. Enter the Partition Name. Create the partition for LDS as cisco.com. Any suitable value can be provided. Click

Next.

Active Directory Lightweight Directory Services Setup Wizard			
Application Directory Partition An application directory partition stores application-specific data.			
Do you want to create an application directory partition for this instance of AD LDS?			
No, do not create an application directory partition			
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.			
Yes, create an application directory partition			
Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name: CN=Partition1,DC=Woodgrove,DC=COM			
Partition name:			
DC=cisco,DC=com			
< <u>B</u> ack <u>N</u> ext > Cancel Help			

8. Choose the default options in subsequent pages and continue.

Active Directory Lightweight Directory Services Setup Wizard			
File Locations You can specify a location for each type of file associated with this instance of AD LDS.			
Specify the locations to store files associated with AD LDS.			
Data files: C:\Program Files\Microsoft ADAM\MultiForest\data Browse			
D <u>a</u> ta recovery files:			
C:\Program Files\Microsoft ADAM\MultiForest\data Browse			
< <u>B</u> ack <u>N</u> ext > Cancel Help			
🔄 🔹 Active Directory Lightweight Directory Services Setup Wizard			
Service Account Selection AD LDS performs operations using the permissions associated with the account you select.			
Set up AD LDS to perform operations using the permissions associated with the following account.			
Instruction of the default Windows service account.			
AD LDS has the permissions of the default windows service account.			
○ <u>I</u> his account:			
AD LDS service has the permissions of the selected account.			
∐ser name:			
Password:			
< <u>B</u> ack <u>N</u> ext > Cancel Help			

Active Directory Lightweight Directory Services Setup Wizard			
AD LDS Administrators You can specify the user or group that will have administrative privileges for this instance of AD LDS.			
Assign the following user or group of users administrative permissions for AD LDS.			
Currently logged on user: CITG2012R2\administrator The user that is installing AD LDS will have administrative permissions for this instance of AD LDS.			
Ihis account The selected user or group will have administrative permissions for this instance of AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.			
Account name:			
< <u>B</u> ack <u>N</u> ext > Cancel Help			

9. Check the MS-InetOrgPerson.LDF, MS-User.LDF, MS-UserProxy.LDF, and MS-UserProxyFull.LDF check boxes. Click Next.

Active Directory Lightwo	eight Directory Services Setup Wizard 🛛 💌		
Importing LDIF Files You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.			
To configure the AD LDS service in a specific way, import one or more of the LDIF files listed below.			
LDIF file name MS-AdamSyncMetadata.LDF MS-ADLDS-DisplaySpecifiers.L MS-AZMan.LDF MS-AZMan.LDF MS-InetOrgPerson.LDF MS-MembershipTransitive.LDF MS-ParentDistname.LDF MS-RepIValMetadataExt.LDF MS-SecretAttributeCABs.LDF MS-SecretAttributeCABs.LDF	Description ADAMSync metadata schema extension. Required for AD LDS Display specifiers schema and display specifiers AD LDS schema extensions for AzMan. AD LDS inetOrgPerson, user and related classes. AD LDS memberhsip transitive. AD LDS parent dist name. AD LDS ReplValueMetaDataExt. AD LDS Secret Attribute Control Access Binbts		
< <u>B</u> ack <u>N</u> ext> Cancel Help			
Importing LDIF Files You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.			
To configure the AD LDS service in a specific way, import one or more of the LDIF files listed below.			
LDIF file name MS-ParentDistname.LDF MS-RepIValMetadataExt.LDF MS-SecretAttributeCARs.LDF MS-SetOwnerBypassQuotaCA MS-UserIDF MS-UserProxy.LDF MS-UserProxyFull.LDF	Description AD LDS parent dist name. AD LDS ReplValueMetaDataExt. AD LDS Secret Attribute Control Access Rights. AD LDS Set Owner and Bypass Quota Control Acces AD LDS user class and related classes. AD LDS simple userProxy class. AD LDS full userProxy class. Requires MS-User.LDF		
< <u>B</u> .	ack <u>N</u> ext > Cancel Help		

10. Click Next in order to start the installation.

	Active Directory Lightweight Directory Services Setup Wizard
I	Ready to Install The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.
	Before continuing, review and confirm your selections.
	Selections:
	Install a unique instance of AD LDS.
	Instance name: MultiForest Computers will connect to this instance of AD LDS using the following ports: LDAP port: 50000 SSL port: 50001
	AD LDS replication will use Negotiate authentication.
	Store AD LDS data files in the following location: \sim
	To change your selections, click Back. To install AD LDS, click Next.
	< <u>B</u> ack <u>N</u> ext > Cancel Help

Ō	Active Directory Lightweight Directory Services Setup Wizard		
Ir	nstalling AD LDS The AD LDS Setup Wizard is installing AD LDS.		
	Installing AD LDS		
Please wait while the wizard completes the following steps. Copied files Starting Active Directory Lightweight Directory Services installation			
	< <u>B</u> ack <u>N</u> ext > Cancel Help		

11. The installation is completed successfully. Click Finish.



Configure ADAM Schema Analyzer

If the user IDs (sAMAccountNames) are unique across different domains and there are not multiple users with the same ID in different domains of different forests, then the users can be synchronized from the AD to the respective forests on the AD LDS, all of which can exist on a single partition on the AD LDS in a **multi forest** setup. For example, consider the figure in the <u>Active Directory Multiple Forest Support Scenario in CUCM</u> section, and if a user ID 'alice' exists in only one of the three domains the setup in this scenario would be as follows:

PARTITION	FOREST	DN
P1	cisco.com	DC=cisco,DC=com
	webex.com	DC=webex, DC=cisco,DC=com
	tandberg.com	DC=Tandberg, DC=cisco,DC=com

In order to configure CUCM with AD LDS, the user ID (sAMAccountName) needs to be unique across all the forests. CUCM currently supports only a single partition in AD LDS.

If the sAMAccountNames are not unique, consider using any of these attributes if they uniquely identify a user account - email, telephoneNumber, employeeNumber, uid, or userPrincipalName.

- 1. Copy the schema from the domain to ADAM.
- 2. Open AD DS/LDS schema analyzer (ADSchemaAnalyzer.exe) in the directory

c:\windows\adam.

3. Choose File > Load targe	et schema.	
AD DS/LDS Schema Analyzer		
File Schema Tools		
Load target schema Ctrl+T		
Load base schema Ctri+B		
Create LDIF File, Ctrl+L		
Exit		
	•	
		<u>^</u>
		-

4. Provide the credentials of the source AD Domain Controller that you want to import from.

Load target so	hema 📃 🗆 🗙
Server[:port]	ad2k8-1
Username	Administrator
Password	
Domain	cisco
Bind type	
Server type -	
Auto	2
C AD DS/LD	s 🔨
C Generic (s	subschemaSubentry)
Load LDIF	Ok Cancel

Click Ok.

5. Choose File > Load base schema.

AD DS/LDS Schema Analyzer		- U ×
File Schema Tools		
Load target schema Ctrl+T		
Load base schema Ctrl+B		
Cre'alle LDIF file Ctrl+L		
Exit		
Validating schema		_
Processing dependencies		
Loaded schema: 1286 attributes, 230 cl	asses, 15 property sets.	
		•

6. Specify the AD LDS to which you want to connect and extend the schema. Click **Ok**. Load base schema

Server[:port]	localhost:50000
Username	
Password	
Domain	
Bind type	Secure C Simple
Server type	
Auto	
C AD DS/LD	S
O Generic (subschemaSubentry)
Load LDIF	Ok Cancel

7. Choose Schema > Mark all non-present elements as included.

AD DS/LDS Schema Analyzer	
File Schema Tools	
Hide present elements	
Show present elements	
Mark alignon-present elements as included	
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;LCRPLORC;;;AU), base D:S:	_
sitesContainer: defaultSecurityDescriptor mismatch: target D:(A;;CCDCLCSWRPWPDTLOCRSDRCWI (A+CCDCLCSWRPWPDTLOCRSDRCWDWO++SY)(A+LCRPLORC++41), have D:S;	DWO:::DA)
subnet: defaultSecurityDescriptor mismatch: target D:(A;:CCDCLCSWRPWPDTLOCRSDRCWDWO;;;	DA)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDW0;;;SY)(A;;LCRPLORC;;;AU), base D:S: expectCentainer: defaultSecurityDescriptor mismatch: target D:(A::CCDCLCSWRPWPLOCRBCWDW(0DA)
(A;:CCDCLCSWRPWPDTLOCRSDRCWDWO;::SY)(A;:LCRPLORC;::AU), base D:S:	
top: default SecurityDescriptor mismatch: target D:(A::CCDCLCSWRPWPDTLOCRSDRCWDWO:::DA)	
user: defaultSecurityDescriptor mismatch: target D:(A::CCDCLCSWRPWPDTLOCRSDRCWDWO:::DA	0
(A::CCDCLCSWRPWPDTLOCRSDRCWDWO:::SY)(A::CCDCLCSWRPWPDTLOCRSDRCWDWO:::A	O)(A::LCRPLORC:::PS)
-11d0-9819-00aa0040529b::PS)(OA::RPWP:77b5b886-944a-11d1-aebd-0000f80367c1::PS)(OA::RPV	VP:e45795b2-9455-11d1-aebd-
0000f80367c1;;PS)(OA;;RPWP;e45795b3-9455-11d1-aebd-0000f80367c1;;PS)(OA;;RP;037088f8-0ae	1-11d2-b422-00a0c968f939;;RS)
(OA;;RP;4c164200-20c0-11d0-a/68-00aa006e0529;;RS)(OA;;RP;6c0ac240-/9a9-11d0-9020-00c04fc (OA::RP:59ba2f42-79a2-11d0-9020-00c04fc2d3cf::AU)(OA::RP:77b5b886-944a-11d1-aebd-0000f803)	.2d4ct;;RS)(A;;RC;;;AU) 67c1::AU)(OA::RP:e45795b3-9455
-11d1-aebd-0000f80367c1;;AU)(OA;;RP;e48d0154-bcf8-11d1-8702-00c04fb96050;;AU)(OA;;CR;ab72	1a53-1e2f-11d0-9819-
100aa0040529b;;WD)(OA;;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;;RS)(OA;;RPWP;6f967a7f-0de 10A::RP:46a9b11d-60ae-405a-b7e84f8a58d456d2::S-1-5-32-560)(OA::RPWP;6db69a1c-9422-11d1-a	(6-11d0-a285-00aa003049e2;;CA) ebd-0000f80367c1::S-1-5-32-561)
(OA;;RPWP;5805bc62-bdc9-4428-a5e2-856a0f4c185e;;S-1-5-32-561), base D:(OA;;CR;ab721a53-1e)	2-11d0-9819-00aa0040529b;;PS)S:
user: systemFlags mismatch: target 16, base 0 Done comparing schemas	
concerning continue.	•

8. Choose File > Create LDIF file. In this example, the file created via this step is diffschema.ldf. In order to simplify the process the file should be created in c:\windows\adam.

AD DS/LDS Schema Analyzer	- O ×
File Schema Tools	
Load target schema Ctrl+T	
Load base schema Ctrl+B	
Create LDIF file Ctrl+L	
Exat	
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;LCRPLORC;;;AU), base D:S:	
subnet: defaultSecurityDescriptor mismatch: target D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;DA) (A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;SY(A;LCRPLORC;;ALI); base D:S;	
subnetContainer: defaultSecurityDescriptor mismatch: target D:(A;;CCDCLCSWRPWPLOCRRCWDWO;;;DA)	
(A;;CCDCLCSWRPWPDTL0CRSDRCWDWO;;;SY)(A;;LCRPL0RC;;;AU), base D:S:	
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;LCRPLORC;;;AU), base D:S:	
user: default SecurityDescriptor mismatch: target D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;DA)	
(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;PS)(OA;;CR;ab721a54-1e2f-11d0-9819-00aa0040529b;;PS)(OA;;CR;ab721a5	56-1e2f
-11d0-9819-00aa0040529b;;PS)(OA;;RPWP;77b5b886-944a-11d1-aebd-0000f80367c1;;PS)(OA;;RPWP;e45795b2-945565666666666666666666666666666666666	bd-
10000780367c1;;;PS)(0A;;;RPWP;;e4579553-9455-1101-aebd-0000780367c1;;PS)(0A;;;RP;03708878-0ae1-1102-6422-00a0c9687938 1(0A;:RP:4c164200-20c0-11d0-a768-00aa006e0529;;RS)(0A;:RP;bc0ac240-79a9-11d0-9020-00c04fc2d4cf;:RS)(A;:RC;::AU)	/;:R5)
(OA::RP:59ba2f42-79a2-11d0-9020-00c04fc2d3cf::AU)(OA::RP:77b5b886-944a-11d1-aebd-0000f80367c1::AU)(OA::RP:e45795b	3-9455
[-11d1-aebd-0000f80367c1;;AU)(OA;;RP;e48d0154-bcf8-11d1-8702-00c04fb96050;;AU)(OA;;CR;ab721a53-1e2t-11d0-9819- [00aa0040529b::WD)(OA::RP:5f202010-79a5-11d0-9020-00c04fc2d4cf::RS)(OA::RPWP:bf967a7f-0de6-11d0-a285-00aa003049e	2-CA)
(OA::RP:46a9b11d-60ae-405a-b7e8ff8a58d456d2::S-1-5-32-560)(OA::RPWP:6db69a1c-9422-11d1-aebd-0000f80367c1::S-1-5-32	2-561)
(OA;;RPWP;5805bc62-bdc9-4428-a5e2-856a0f4c185e;;S-1-5-32-561), base D:(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b user: systemFlags mismatch: target 16, base 0	s::PS)S:
Done comparing schemas.	
Validating schema	
	•

An option available to help organize the files that need to be generated is to create a separate directory in order to allow for these files to be separated from the main c:\windows\adam directory. Open a command prompt and create a log directory in

c:\windows\adam.cd \windows\adam mkdir logs

9. Import the Idif schema, created with ADSchema Analyzer, to AD LDS. ldifde -i -s localhost:50000 -c CN=Configuration,DC=X

#ConfigurationNamingContext -f diff-schema.ldf -j c:\windows\adam\logs Refer to Using LDIFDE to import and export directory objects to Active Directory for additional Idifde options and command formats.

a Administrator: C:\Windows\system32\cmd.exe
C:\Windows\ADAM>ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #Configura tionNamingContext -f diff-schema.ldf -j c:\windows\adam\logs Connecting to "localhost:50000" Logging in as current user using SSPI Importing directory from file "diff-schema.ldf" Loading entries.
1163 entries modified successfully.
The command has completed successfully
C:\Windows\ADAM>_

Extend the AD LDS Schema with the User-Proxy Objects

The object for the proxy authentication needs to be created and the object class 'user' will not be used. The object class that is created, userProxy, is what allows the bind redirection. The object class detail needs to be created in a ldif file. The file is a creation of a new file, which in this example is MS-UserProxy-Cisco.ldf. This new file is generated from the original MS-UserProxy.ldf and edited, use a text edit program, to have this content:

```
#_____
# @@UI-Description: AD LDS simple userProxy class.
#
# This file contains user extensions for default ADAM schema.
# It should be imported with the following command:
# ldifde -i -f MS-UserProxy.ldf -s server:port -b username domain password -k -j . -c
"CN=Schema, CN=Configuration, DC=X" #schemaNamingContext
#
dn: CN=User-Proxy, CN=Schema, CN=Configuration, DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: classSchema
cn: User-Proxy
subClassOf: top
governsID: 1.2.840.113556.1.5.246
schemaIDGUID:: bxjWYLbzmEiwrWU1r8B2IA==
rDNAttID: cn
showInAdvancedViewOnly: TRUE
adminDisplayName: User-Proxy
adminDescription: Sample class for bind proxy implementation.
objectClassCategory: 1
lDAPDisplayName: userProxy
systemOnly: FALSE
possSuperiors: domainDNS
possSuperiors: organizationalUnit
possSuperiors: container
possSuperiors: organization
defaultSecurityDescriptor:
D:(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;PS)S:
defaultHidingValue: TRUE
```

defaultObjectCates	<pre>gory: CN=User-Proxy,CN=Schema,CN=Configuration,DC=X</pre>
systemAuxiliaryCla	ass: msDS-BindProxy
systemMayContain:	userPrincipalName
systemMayContain:	givenName
systemMayContain:	middleName
systemMayContain:	sn
systemMayContain:	manager
systemMayContain:	department
systemMayContain:	telephoneNumber
systemMayContain:	mail
systemMayContain:	title
systemMayContain:	homephone
systemMayContain:	mobile
systemMayContain:	pager
systemMayContain:	msDS-UserAccountDisabled
systemMayContain:	samAccountName
systemMayContain:	employeeNumber
systemMayContain:	initials
systemMayContain:	ipPhone
systemMayContain:	displayName
systemMayContain:	msRTCSIP-primaryuseraddress
systemMayContain:	uid
dn:	
changetype: modify	Y
add: schemaUpdate	Now
schemaUpdateNow: 3	1

Save MS-UserProxy-Cisco.ldf file in C:\windows\adam.

Import the new object class to AD LDS.

```
ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #ConfigurationNamingContext -f
MS-UserProxy-Cisco.ldf -j c:\windows\adam\logs

Administrator: C:\Windows\system32\cmd.exe
C:\Windows\ADAM>ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-UserProxy-Cisco.ldf -j c:\windows\adam\logs
Connecting to "localhost:50000"
Logging in as current user using SSPI
Importing directory from file "MS-UserProxy-Cisco.ldf"
Loading entries...
2 entries modified successfully.
The command has completed successfully
C:\Windows\ADAM>_
```

Import the Users From AD DC to AD LDS

The user from each domain now needs to be imported to AD LDS. This step needs to be repeated for each domain that needs to synchronize. This example only shows the process against one of

the domains. Start with the original MS-AdamSyncConf.xml and create an XML file for each domain that needs to be synchronized and modify the file with the details specific to each domain to have this content:

```
<?xml version="1.0"?>
<doc>
<configuration>
<description>Adam-Syncl</description>
 <security-mode>object</security-mode>
 <source-ad-name>ad2k8-1</source-ad-name>
<source-ad-partition>dc=cisco,dc=com</source-ad-partition>
<source-ad-account></source-ad-account>
<account-domain></account-domain>
<target-dn>dc=cisco,dc=com</target-dn>
 <query>
  <base-dn>dc=cisco,dc=com</base-dn>
   <object-filter>
(|(&(!cn=Administrator)(!cn=Guest) (!cn=ASPNET)
(!cn=krbtgt)(sAMAccountType=805306368))(&(objectClass=user)(isDeleted=TRUE)))
    </object-filter>
  <attributes>
   <include>objectSID</include>
   <include>mail</include>
   <include>userPrincipalName</include>
   <include>middleName</include>
   <include>manager</include>
   <include>givenName</include>
   <include>sn</include>
   <include>department</include>
   <include>telephoneNumber</include>
   <include>title</include>
   <include>homephone</include>
   <include>mobile</include>
   <include>pager</include>
   <include>msDS-UserAccountDisabled</include>
   <include>samAccountName</include>
   <include>employeeNumber</include>
<include>initials</include>
<include>ipPhone</include>
<include> displayName</include>
<include> msRTCSIP-primaryuseraddress</include>
<include>uid</include>
  <exclude></exclude>
 </attributes>
 </query>
 <user-proxy>
   <source-object-class>user</source-object-class>
   <target-object-class>userProxy</target-object-class>
 </user-proxy>
 <schedule>
 <aging>
   <frequency>0</frequency>
   <num-objects>0</num-objects>
 </aging>
 <schtasks-cmd></schtasks-cmd>
 </schedule>
 </configuration>
 <synchronizer-state>
 <dirsync-cookie></dirsync-cookie>
 <status></status>
 <authoritative-adam-instance></authoritative-adam-instance>
 <configuration-file-guid></configuration-file-guid>
 <last-sync-attempt-time></last-sync-attempt-time>
```

```
<last-sync-success-time></last-sync-success-time>
<last-sync-error-time></last-sync-error-string>
<last-sync-error-string></last-sync-error-string>
<consecutive-sync-failures></consecutive-sync-failures>
<user-credentials></user-credentials>
<runs-since-last-object-update></runs-since-last-object-update>
<runs-since-last-full-sync></runs-since-last-full-sync>
</synchronizer-state>
</doc>
```

In this file, these tags should be replaced to match the domain:

- <source-ad-name> Use the host name of the domain.
- <*source-ad-partition*> Use the root partition from the source AD DC that you want to import from (for example, dc=Cisco, dc=com, or dc=Tandberg, dc=com).
- <base-dn> Choose the container from which to import from. For example, if all users of the domain are required this should be the same as <source-ad-partition>, but if users are from a specific organizational unit (such as Finance OU), it should be similar to OU=Finance, DC=Cisco, DC=com.

Refer to Search Filter Syntax for more information on how to create an <object-filter>.

Save the newly created XML file in C:\windows\adam.

Open a command window, cd \windows\adam.

Enter the command, ADAMSync /install localhost:50000 c:\windows\ADAM\AdamSyncConf1.xml /log c:\windows\adam\logs\install.log.

Verify that the file AdamSyncConf1.xml is the newly created XML file.

Synchronize the users with the command **ADAMSync /sync localhost:50000** "dc=cisco,dc=com" /log c:\windows\adam\logs\sync.log.

The result should be similar to:

C:\Windows\ADAM>ADAMSync /sync localhost:389 "dc=cisco.dc=net" /log -Adamsync.exe v1.0 (6) Establishing connection to target server localhost:389. Saving Configuration File on DC=cisco.DC=net Saved configuration File. ADAMSync is querying for a writeable replica of ad0a.cisco.net. Error: DCLocator call failed with error 1355. Attempting to bind directly to str ing. Establishing connection to source server ad0a.cisco.net:389. Using file .\damD360.tmp as a store for deferred dn=references. Populating the schema cache Populating the well known objects cache Starting synchronization run from dc=cisco.dc=net. Starting DirSync Search with object mode security. Updating the configuration file DirSync cookie with a new value. Beginning processing of deferred dn references. Finished processing of deferred dn references. Finished processing of deferred dn references. Finished successful) synchronization run. Number of entrics processed via ldirSync: 0 Number of object additions: 0 Number of object deletions: 0 Number of object deletions: 0 Number of object tenames: 0 Number of object tenames: 0 Number of references processed / dropped: 0. 0 Maximum number of attributes seen on a single object: 0 Maximum number of attributes seen on a single object: 0 Maximum number of values retrieved via range syntax: 0 Beginning aging run. Aging requested every 0 runs. We last aged 2 runs ago. Saving Configuration file.

In order to complete an automatic sync from AD to ADAM , use the Task scheduler in Windows.

Create a .bat file with this content in it:

"C:\Windows\ADAM\ADAMSync" /install localhost:50000 c:\windows\ADAM\AdamSyncConf1.xml /log c:\windows\adam\logs\install.log

"C:\Windows\ADAM\ADAMSync" /sync localhost:50000 "dc=cisco,dc=com" /log c:\windows\adam\logs\syn.log

Schedule the task to run the .bat file as and when required. This takes care of additions, modifications, and deletions that happen in AD to be reflected in ADAM as well.

You can create another .bat file and schedule it to complete an automatic sync from the other forest.

Create the User in AD LDS for CUCM Synchronization and Authentication

- 1. Open ADSI Edit from the Administrator tools in the Startup menu.
- 2. Choose File > Connection (or Action > Connect To).
- 3. Connect to base dn of the AD LDS tree (DC=Cisco,DC=com) and specify the host and port where it is hosted (localhost:50000). Click **OK**.

🔏 ADSI Edit	
File Action View Help	
🗢 🔿 🔲 🖸 🚺 🖬	
Z ADSI Edit	Welcome to ADSI Edit Active Directory Services Interfaces Editor (ADSI Edit) is a low-level editor for Ac Directory Domain Services / Active Directory Lightweight Directory Services. It al to view, modify, create, and delete any object in Microsoft's AD DS/LDS.
Con	nection Settings 🛛 🔀 🕻 To.
Na	me: Multiforest
Pal	th: LDAP://localhost:50000/dc=cisco,dc=com
LC C	onnection Point
	Select or type a Distinguished Name or Naming Context:
	dc=cisco,dc=com
	C Select a well known Naming Context:
	Default naming context
	omputer
	Select or type a domain or server: (Server Domain [:port])
	localhost:50000
	Default (Domain or server that you longed in to)
	Use SSL-based Encryption
A	dvanced OK Cancel

4. Right-click the base DN and choose **New > Object**.

📝 ADSI Edit				
File Action View Help				
🗢 🔿 🔰 📅 🗶 🖻 🧕 🕫	÷ 🛛 📅			
2 ADSI Edit	Name	Class	Distinguished Name	Actions
MultiForest [localhost:50000] Image: Contemporation of the second sec	CN=LostAndFound	lostAndFound msDS-Quota	CN=LostAndFound,DC=clsco,DC=com CN=NTDS Ountas DC=clsco,DC=com	DC=cisco,dc=com
New	Cbject	container	CN=Roles,DC=cisco,DC=com	More Actions
View	• °			
Rename Refresh Export List				
Properties				
Help				
Consta a new object	<u>[4</u>			
create a new object				

5. Choose user. Click Next.

Create Object	×
Colorto door	
Select a class:	
msMQ-Custom-Recipient mSMQMigratedUser msPKI-Key-Recovery-Agent organization organizationalUnit physicalLocation orintQueue	•
remoteMailRecipient rFC822LocalPart rpcContainer samServer	
IuserProvv Kg	
< Back Next >	Cancel Help

6. In the Value field, enter the chosen object name. In this example "root" is the chosen name (any name could be chosen here). Click **Next**.

Create Object	<u>×</u>	4
Attribute:	cn	
Syntax:	Unicode String	
Description:	Common-Name	
Value:	root	
	< Park Next > Cancel Hala	
	< Back Next > Cancel Help	

7. In order to provide a password to the new user, right-click the user and choose **Reset Password**

ADSI Edit				_ 0 >
File Action View Help				
🗢 🔿 🖄 📷 🗙 🚍 🙆 😖				
2 ADSI Edit	Name	Class	Distinguished Name	Actions
MultForest [locahost: 50000]	CN=LostAndFound	lostAndFound	CN=LostAndFound,DC=cisco,DC=com	DC=cisco,dc=com
CN=LostAndFound	CN=Roles	container	CN=Roles,DC=dsco,DC=com	More Actions
CN=NTDS Quotas	Move Move		CN=root,dc=cisco,dc=com	CII=root -
CN-root	New Connection from He Reset Password New Delete Rename Refresh Properties Help	re		More Actions

8. The new user is disabled by default. In order to enable the new user, right-click the user and choose **Properties**.



9. Browse to the attribute msDS-UserAccountDisabled and click Edit.

mail <not set="">manager<not set="">middleName<not set="">mobile<not set="">mS-DS-ConsistencyC<not set="">msDS-ConsistencyG<not set="">msDS-UserAccountDiTRUEmsDS-UserDontExpir<not set="">ms-DS-UserEncrypte<not set="">ms-DS-UserPassword<not set="">namerootntPwdHistory<not set="">o<not set="">objectCategoryCN=Person,CN=Schema,CN=Configuration,C</not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>	Attribute	Value
manager <not set="">middleName<not set="">mobile<not set="">mS-DS-ConsistencyC<not set="">msDS-UserAccountDiTRUEmsDS-UserDontExpir<not set="">ms-DS-UserEncrypte<not set="">ms-DS-UserPassword<not set="">namerootntPwdHistory<not set="">o<not set="">objectCategoryCN=Person,CN=Schema,CN=Configuration,C</not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>	mail	<not set=""></not>
middleName <not set="">mobile<not set="">mS-DS-ConsistencyC<not set="">mS-DS-ConsistencyG<not set="">msDS-UserAccountDiTRUEmsDS-UserDontExpir<not set="">ms-DS-UserEncrypte<not set="">ms-DS-UserPassword<not set="">namerootntPwdHistory<not set="">o<not set="">o<not set="">objectCategoryCN=Person,CN=Schema,CN=Configuration,C</not></not></not></not></not></not></not></not></not></not>	manager	<not set=""></not>
mobile <not set="">mS-DS-ConsistencyC<not set="">mS-DS-ConsistencyG<not set="">msDS-UserAccountDiTRUEms-DS-UserDontExpir<not set="">ms-DS-UserEncrypte<not set="">ms-DS-UserPassword<not set="">namerootntPwdHistory<not set="">o<not set="">o<not set="">o<not set="">objectCategoryCN=Person,CN=Schema,CN=Configuration,C</not></not></not></not></not></not></not></not></not></not>	middleName	<not set=""></not>
mS-DS-ConsistencyC <not set=""> mS-DS-ConsistencyG <not set=""> msDS-UserAccountDi TRUE msDS-UserDontExpir <not set=""> ms-DS-UserEncrypte <not set=""> ms-DS-UserPassword <not set=""> name root ntPwdHistory <not set=""> o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not></not></not></not></not></not></not>	mobile	<not set=""></not>
mS-DS-ConsistencyG <not set=""> msDS-UserAccountDi TRUE msDS-UserDontExpir <not set=""> ms-DS-UserEncrypte <not set=""> ms-DS-UserPassword <not set=""> name root ntPwdHistory <not set=""> o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not></not></not></not></not></not>	mS-DS-ConsistencyC	<not set=""></not>
msDS-UserAccountDi TRUE msDS-UserDontExpir <not set=""> ms-DS-UserEncrypte <not set=""> ms-DS-UserPassword <not set=""> name root ntPwdHistory <not set=""> o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not></not></not></not></not>	mS-DS-ConsistencyG	<not set=""></not>
msDS-UserDontExpir <not set=""> ms-DS-UserEncrypte <not set=""> ms-DS-UserPassword <not set=""> name root ntPwdHistory <not set=""> o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not></not></not></not></not>	msDS-UserAccountDi	TRUE
ms-DS-UserEncrypte <not set=""> ms-DS-UserPassword <not set=""> name root ntPwdHistory <not set=""> o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not></not></not></not>	msDS-UserDontExpir	<not set=""></not>
ms-DS-UserPassword <not set=""> name root ntPwdHistory <not set=""> o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not></not></not>	ms-DS-UserEncrypte	<not set=""></not>
name root ntPwdHistory <not set=""> o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not></not>	ms-DS-UserPassword	<not set=""></not>
ntPwdHistory <not set=""> o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not></not>	name	root
o <not set=""> objectCategory CN=Person,CN=Schema,CN=Configuration,C</not>	ntPwdHistory	<not set=""></not>
objectCategory CN=Person,CN=Schema,CN=Configuration,C	0	<not set=""></not>
	objectCategory	CN=Person,CN=Schema,CN=Configuration,C

10. Click the **False** radio button in order to enable the user account. Click **OK**.

Attribute Editor	1 Volue
Attribute	
manager	
middle Boolean Attr	ibute Editor
mS-DS Attribute: mS-DS Value: msDS- msDS- ms-DS False ms-DS Value:	msDS-UserAccountDisabled
name ntPwd	OK Cancel
o objectCategory	CN=Person,CN=Schema,CN=Configuration,C
Edit	Filter

11. Click the **True** radio button in order to ensure the password will never expire. Click **OK**.

CN=root Properties		? ×
Attribute Editor		
Attributes:		
Attribute	Value	<u> </u>
msDS-PhoneticDispla	<not set=""></not>	
msDS-PhoneticFirstN	<not set=""></not>	
msDS: Boolean Attrit	oute Editor 🛛 🔀	
msDS- Attribute:	msDS-UserDontExpirePassword	
msDS- Value:		
msDS- True		
msDS- C False		
ms-DS C Not set		
ms-DS	OK Cancel	
msExc		
msExchLabeledUBI	<not set=""></not>	
		- -
		<u> </u>
Edit	Filt	er
ОК	Cancel Apply	Help

The new user needs to be added to one group that has reading permission to the AD LDS, which in this example Administrators was chosen. Browse to CN=Roles > CN=Administrators. Right-click CN=Administrators and choose Properties.



13. Choose the attribute member and click Edit.

F F	ADST Edit IN=Administrators Prope Attribute Editor	erties ?×
5	Attributes:	
E	Attribute	Value
	garbageCollPeriod	<not set=""></not>
	group.Attributes	<not set=""></not>
	groupMembershipSAM	<not set=""></not>
	groupType	0x80000002 = (ACCOUNT_GROUP SECU
	info	<not set=""></not>
	instance Type	0x4 = (WRITE)
	isCriticalSystemObject	TRUE
	isDeleted	<not set=""></not>
	labeledURI	<not set=""></not>
	last Known Parent	<not set=""></not>
		<not set=""></not>
	mail	<not set=""></not>
	member	CN-mot DC-cisco DC-com: CN-Administrate
	member	
	Edit	Filter
	ОК	Cancel Apply Help
•		

14. Enter the new DN that was created previously, **cn=root,dc=Cisco,dc=com**, to this group. Click **OK**.

Μ	ulti-valued Distinguisl	ed Name With Security Principal Editor		x
	Attribute: membe Values:	er		
	Name	Container	Distinguished Name / SID	
	Administrators	/{3E40F477-C577-4F12-BE5A-74B553CD0E8 Add Distinguished Name (DN) Enter a distinguished name (DN) for an obje cn=root,dc=cisco,dc=com OK	CN=Administrators,CN=Roles,CN	
	Add Windows Account.	· _	Remove	
	Add DN		OK Cancel	

15. Choose Update Schema Now and restart AD LDS.

📝 A	DSI Edit					
Fie	Action Vie	ew Help				
(🔶 🖄 📅	0 💩 👔	11			
24	DSI Edit		Name	Class	Distinguished Name	Actions
Ξ	MultiFore	Settings	C=cisco,dc=com	domainDNS	dc=cisco,dc=com	MultiForest [localhost:500 🔺
L '	•	Remove Update Schema N	low			More Actions
	c	New	•			
	- D 🚞 🗉	View	•			
	🗉 🧮 d	Rename				
B	ad2k8-1	Refresh				
	Configure_	Export List				
		Help				
-						
Force	the schema ca	sche to be flushed.				

🏭 Server Manager			_ 🗆 🗵
File Action View Help			
💠 🐟 🖄 📆 📆			
Server Manager (AD2K8-1)	Active Directory Lightweight Directory Services		
Roles Roles Roles Roles Roles			
Active Directory Lightweigh	Provides a store for application-specific directory data.		
∃ B DNS Server III and Eeabures			
E Diagnostics	Summary		-
Configuration			_
in El conste	(i) Events: 4 informational in the last 24 hours	Go to Event Viewer	
	√ 4 Events	Her Events	
	Level Event ID Date and Time Source	Properties	
	Dinformation 701 11/2/2009 5:03:17 PM ADAM [Mu	EE HICE AI EVENIS	
	(i) Information 701 11/2/2009 5:03:17 PM ADAM [NU		
	Dinformation 700 11/2/2009 5:03: 17 AM ADAM [Mu		
]	
	System Services: Al Running	Go to Services	
	Display Name Service Name Status Startup Type Monitor	🔄 Preferences	
	MultForest ADAM_MultFo Running Auto Yes	Stop	
	Provide and Provid	Start	
	Description:	I Restert	
	⊗ Advanced Tools		
	Create a new AD LDS instance	AD LDS Setup Wizard	
	Query, view, and edit objects and attributes in the directory	📑 ADGI Edit	
	Perform LDAP operations against the directory such as connect, bind, search, modify, add, and delete	Ldp.exe	
4 NOR 1	Q Last Refresh: 11/2/2009 6:04:25 PM Configure refresh		
	,		

Configure Bind Redirection

By default, binding to ADAM with bind redirection requires an SSL connection. SSL requires the installation and use of certificates on the computer that runs ADAM and on the computer that connects to ADAM as a client. If certificates are not installed in your ADAM test environment, you can disable the requirement for SSL as an alternative.

By default, SSL is enabled. In order to make the LDAPS protocol work in ADAM/LDS you will need to generate a certificate.

In this example, the Microsoft Certification Authority Server is used in order to issue the certificate. In order to request a certificate, go to the web page of the Microsoft CA - http://<MSFT CA hostname>/certsrv and complete these steps:

- 1. Click Request a certificate.
- 2. Click Advanced certificate request.
- 3. Click Create and submit a request to this CA.
- 4. In the Name textbox, enter the full DNS name of the ADAM/AD LDS server.
- 5. Ensure Type of certificate is Server authentication certificate.
- 6. For the format, choose PCKS10.
- 7. Choose Mark Keys as exportable.
- 8. Optionally, fill in the other information.
- 9. In the Friendly name textbox, enter the full dns name of the ADAM/AD LDS server.
- 10. Click **Submit**.

Go back to the certification authority interface and click the Pending Certificates folder. Right-

click the certificate request made by the ADAM/AD-LDS machine and issue the certificate.

The certificate has now been created and resides in the "Issued certificates" folder. Next , you need to download and install the certificate:

- 1. Open http://<MSFT CA hostname>/certsrv.
- 2. Click View the status of a pending certificate request.
- 3. Click the certificate request.
- 4. Click the certificate in order to install it.

In order to let the ADAM service use the certificate, you need to put the certificate in the ADAM service's personal store:

- 1. From the Start menu, choose **Run**. Type **mmc**. This opens the managment console.
- 2. Click File \ Add/Remove snap-in.
- 3. Click Add and choose Certificates.
- 4. Chose Service account.
- 5. Choose **Local computer**.
- 6. Choose your ADAM instance service.
- 7. Add a new Certificate snap-in, but this time choose **My user account** instead of Service account.
- 8. Click Close and click Ok.
- 9. In the Certificates Current user-tree, open the Personal folder.
- 10. Select the certificate and copy it into the same location under "Certificates *adam instance name*".

In order to grant Read permission on the server authentication certificate to the Network service account, complete these steps:

- 1. Navigate to this default directory where the installed or imported certificates are stored C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.
- 2. Right-click the appropriate server authentication certificate. Click Properties.
- 3. Click the Security tab. Click Edit.
- 4. In the **Permissions** dialog box, click **Add**.
- 5. In the Select Users, Computers, or Groups dialog box, enter Network Service. Click OK.
- 6. Restart your ADAM instance.

More information can be found in <u>Appendix A: Configuring LDAP over SSL Requirements for AD</u><u>LDS</u>.

Next, upload the certificate of the CA that issued the certificate to the ADAM/AD LDS machine as a CUCM directory trust.

Refer to the <u>Cisco Unified Communications Operations System Administration Guide</u> for additional details.

Choose the checkbox in order to use SSL in LDAP Directory page and LDAP Authentication page.

Enter 50001 (in this example) for the LDAP port, which is the SSL port number given when you installed the ADAM/AD LDS instance.

In order to disable the SSL requirement for bind redirection, complete these steps:

- 1. Click Start, point to Administrative Tools, and click ADSI Edit.
- 2. On the Action menu, choose Connect to.
- 3. In the Computer field, enter **localhost:50000** (this is theADAM host and port.).

mneci	tion settings	
Vame:	Configuration	
Path:	LDAP://localhost:50000/Configuration	
Conne	nection Point	
C s	Select or type a Distinguished Name or Namir	ng Context:
		_
Θs	Select a well known Naming Context:	
	Configuration	•
Comp	puter	
• s	Select or type a domain or server: (Server	Domain [:port])
	localhost: 50000	•
C D	Default (Domain or server that you logged in	to)
Πu	Use SSL-based Encryption	
		- I (
Advar	inced OK	Cancel

- 4. In the Connection Point section, click the **Select a well-known Naming Context** radio button. From the drop-down list, choose **Configuration**. Click **OK**.
- 5. In the console tree, browse to this container object in the configuration partition: CN=Directory Service,CN=Windows NT,CN=Services.
- 6. Right-click **CN=Directory Service** and choose **Properties**.

 Configuration [localhost: 50000] CN=Configuration, CN={48E9D889- CN=DirectoryUpdates CN=DisplaySpecifiers CN=Extended-Rights CN=ForeignSecurityPrincipals CN=LostAndFoundConfig CN=Partitions CN=Pales 	-DFS	
CN=Services		
CN=Sites	New Connection from Here	
	New	•
	View	•
Opens the properties dialog box for the curr	Delete Rename Refresh Export List	
Jystem System	Properties	
1 item selected	Help	

- 7. In Attributes, click msDS-Other-Settings. Click Edit.
- 8. In Values, click **RequireSecureProxyBind=1** and then click **Remove**.
- 9. In Value to add, enter RequireSecureProxyBind=0, click Add, and then click OK.
- 10. Restart AD LDS for the changes to take effect.

Configure CUCM

ADAM/AD LDS synchronization and authentication is supported in CUCM Version 9.1(2) and later.

- 1. Choose **System > LDAP > LDAP System**.
- 2. Select Microsoft ADAM or Lightweight Directory Services.
- 3. You can choose any of these LDAP userid attributes: mail, employee Number, or telephone Number. uid is only used with standalone ADAM/AD LDS and not with AD multi-forest support.

oliolo Cisco Un Cisco For Cisco Uni	ified CM Administration fied Communications Solutions		
System 👻 Call Routing 👻 M	edia Resources 🔻 Advanced Features 👻 Device 💌	Application 🔻	User Mar
LDAP System Configurat	ion		
Save			
Status Status: Ready			
LDAP System Informatio			
Enable Synchronizing fr	om LDAP Server		
LDAP Server Type	Microsoft ADAM or Lightweight Directory Services	•	
LDAP Attribute for User ID	mail	•	
Save			

Currently, for LDAP Server type "Microsoft ADAM or Lightweight Directory Services" mode, samAccountName is not included in the LDAP Attribute for Userid drop-down . The reason is that it is not an attribute supported with standalone ADAM/AD LDS. If the CUCM UserID mapped to sAMAccountName needs to be used then that agreement should be configured as AD

AD.					
cisco	Cisco Un For Cisco Uni	ified CM Ad	Iministration ations Solutions	י	
System 👻	Call Routing 👻 M	ledia Resources 👻	Advanced Features 👻	Device 👻	Application 👻
LDAP Sys	tem Configurat	ion			
I Pleas	e Delete All LDA	P Directories Befor	re Making Changes (on This Page	
LDAP Sys	tem Informatio	on ———			
🗹 Enable	Synchronizing fr	rom LDAP Server			
LDAP Ser	ver Type	Microsoft Active (Directory		-
LDAP Attr	ibute for User ID	sAMAccountName	e		-

4. Configure LDAP synchronization with the credentials of the user created in AD LDS.

System ▼ Call Routing ▼ Media Reso	urces 🔻 Adv	anced reatures 👻	Device V Application	Oser Management	Juk Auministration ▼ Theip) 🔻
LDAP Directory					Related Links: Back t	to LDAP Directory Find
🔜 Save						
- IDAR Directory Information						
LDAP Configuration Name*	Multiforest					
LDAP Manager Distinguished Name*	* cn=root.dc=	=cisco.dc=com				
LDAP Password*		•				
Confirm Password*						
LDAP User Search Base*	de=cisco de	=000				
LDAP Custom Filter	CustomFilte	er		*		
- LDAP Directory Synchronizatio	n Schedule -					
Perform Sync Just Once						
Perform a Re-sync Every*	7		DAY 🔽			
Next Re-sync Time (YYYY-MM-DD hł	h:mm)* 2010)-01-20 00:00				
– User Fields To Be Synchronize	d ———					
Cisco Unified Communications Manag	ger User Fields	5 LDAP User Fie	lds	Cisco Unified Communio	ations Manager User Fie	lds LDAP User Fields
User ID Middle Name		mail		First Name		givenName
		middleName				
Phone Number		manager	ahay y	Mail ID		gepartment
		telephoneNum	nber 🚩	Field ID		mail 💌
LDAP Server Information						
Host Name or IP Address for	Server*			LDAP Port* Use S	\$L.	
172.18.36.240				50000		
Add Another Red	lundant LDA	P Server				
-						
			_			
[Save]				<u> </u>		
Save) Configure LDAP auth	nenticati	ion with tl	he credentials	s of the user cr	eated in AD L	.DS.
Configure LDAP auth	nenticati	ion with tl	he credentials	s of the user cr	eated in AD L	DS.
Configure LDAP auth	nenticati Jnifie	ion with th d CM A	he credentials	s of the user cr tion	eated in AD L	.DS.
Configure LDAP auth	nenticati J nifie d	ion with th d CM A	he credentials dministra cations Solutio	s of the user cr tion ns	eated in AD L	.DS.
Save Configure LDAP auth Cisco For Cisco System - Call Routing -	nenticati Jnified Unified (Media Re	on with the discrete state of the discrete state state of the discrete state of the disc	he credentials dministra dministra cations Solutio	s of the user cr tion ns Device - Applicat	eated in AD L ion - User Mana	.DS. agement ▼ Bulk /
Save Configure LDAP auth Cisco System Call Routing Cisco	nenticati Jnified Unified (Media Re	ion with the distance of the d	he credentials dministra dministra cations Solutio Voice Mail 🗸	s of the user cr tion ns Device - Applicat	eated in AD L ion → User Mana	.DS. agement ▼ Bulk /
Save Configure LDAP auth Cisco For Cisco System Call Routing LDAP Authentication	nenticati Jnified Unified (Media Re	ion with the distance of the d	he credentials dministra ations Solutio Voice Mail •	s of the user cr tion ns Device Applicat	eated in AD L ion ▼ User Mana	DS. agement ▼ Bulk /
Save Configure LDAP auth Cisco System Call Routing LDAP Authentication	nenticati Jnified Unified (Media Re	on with the distance of the di	he credentials dministra ations Solutio Voice Mail 🗸	s of the user cr tion ns Device - Applicat	eated in AD L ion	.DS. agement マ Bulk /
Save Configure LDAP auth Cisco System Call Routing Cisco LDAP Authentication	nenticati Unified Media Re	ion with the discrete state of the discrete	he credentials dministra dministra cations Solutio Voice Mail 🗸	s of the user cr tion ns Device - Applicat	eated in AD L ion	.DS. agement ▼ Bulk /
Save Configure LDAP auth Cisco Cisco System Call Routing LDAP Authentication Save	nenticati Jnified Unified (Media Re	ion with the d CM A Communic esources -	he credentials dministra ations Solutio Voice Mail 🗸	s of the user cr tion ns Device - Applicat	eated in AD L ion	.DS. agement
Save Configure LDAP auth Cisco System Call Routing Cisco System Call Routing Call	nenticati Jnified Unified (Media Re	ion with the distance of the d	he credentials dministra ations Solutio Voice Mail •	s of the user cr tion ns Device - Applicat	eated in AD L ion	.DS. agement
Save Configure LDAP auth Cisco System Call Routing Cisco System Call Routing Call	nenticati Jnified Unified (Media Re	on with the distance of the di	he credentials dministra ations Solutio Voice Mail •	s of the user cr tion ns Device Applicat	eated in AD L ion	.DS. agement ▼ Bulk /
Save Configure LDAP auth Cisco Cisco System ▼ Call Routing ▼ LDAP Authentication Save Save Status: Ready	nenticati Unified (Media Re	on with the distance of the di	he credentials dministra cations Solutio Voice Mail 🗸	s of the user cr tion ns Device - Applicat	eated in AD L ion - User Mana	.DS. agement ▼ Bulk A
Save Configure LDAP auth Cisco Cisco System ▼ Call Routing ▼ LDAP Authentication Save Status Status: Ready	nenticati Unified Media Re	ion with the diameter of the d	he credentials dministra cations Solutio Voice Mail 🗸	s of the user cr tion ns Device - Applicat	eated in AD L ion	.DS. agement
Save Configure LDAP auth Cisco System Call Routing Cisco System Call Routing Cisco System Call Routing Cisco System Status Call Routing Cisco Status Call Routing Cisco Call Routing Cisco System Status Call Routing Cisco Call Routing Cisco System Call Routing Cisco System Status Call Routing Cisco Cisco Cisco Status Call Routing Cisco Cisco Cisco Status Call Routing Cisco Cisco Cisco	nenticati Unified Media Re	on with the dominant of the do	he credentials dministra cations Solutio Voice Mail •	s of the user cr tion ns Device - Applicat	eated in AD L ion	DS. agement Bulk /
Save Configure LDAP auth Cisco Cisco For Cisco System ▼ Call Routing ▼ LDAP Authentication Save Status Other Status: Ready LDAP Authentication Status: Use LDAP Authentication	nenticati Unified Media Re for End	on with the diagram of the diagram o	he credentials dministra cations Solutio Voice Mail •	s of the user cr tion ns Device - Applicat	eated in AD L ion	.DS. agement ▼ Bulk /
Save Configure LDAP auth Cisco Cisco System ▼ Call Routing ▼ LDAP Authentication Save Status Other Status Status: Ready LDAP Authentication Image: Status: Ready Use LDAP Authentication Image: Distingui	nenticati Unified Media Re Media Re	Users	he credentials dministra cations Solutio Voice Mail Voice Mail	s of the user cr tion ns Device - Applicat	eated in AD L ion - User Mana	.DS. agement Bulk /
Save Configure LDAP auth Cisco Cisco System ▼ Call Routing ▼ LDAP Authentication Save Status Other Status Other Status Other Status Other Status Other Status DAP Authentication ✓ Use LDAP Authentication ✓ Use LDAP Authentication ✓ LDAP Password*	nenticati Unified Media Re for End ation for E	Users ind Users ind Users ind Users	he credentials dministra ations Solutio Voice Mail •	s of the user cr tion ns Device - Applicat	eated in AD L	DS. agement ▼ Bulk /
Save Configure LDAP auth Cisco Cisco System ▼ Call Routing ▼ LDAP Authentication Save Status Save Cisco For Cisco Visco System ▼ Call Routing ▼ Coll Routing ▼ For Cisco For Cisco System ▼ Call Routing ▼ Coll Routing ▼ Coll Routing ▼ Confirm Password *	nenticati Unified Media Re for End ation for E ished Nam	ion with the communication of	he credentials dministra cations Solutio Voice Mail •	s of the user cr tion ns Device - Applicat	eated in AD L	.DS. agement
Save Configure LDAP auth Cisco System ▼ Call Routing ▼ LDAP Authentication Save Status Cisco System ▼ Call Routing ▼ LDAP Authentication Save Cisco Superior Cisco System ▼ Call Routing ▼ LDAP Authentication Save Cisco Superior Cisco Superior Cisco System ▼ Call Routing ▼ LDAP Authentication Save Cisco Superior Cisco Superior Cisco Superior Cisco Superior Cisco Superior Cisco Superior Cisco Superior Cisco Superior Cisco Cisco Superior Cisco Superior Cisco	nenticati Unified (Media Re for End ation for E ished Nam	Users ind Users ind Users ind Users ind Users	he credentials dministra cations Solutio Voice Mail Voice Mail Voice Mail	s of the user cr tion ns Device - Applicat	eated in AD L	.DS. agement → Bulk /

-LDAP Server Information						
Host Name or IP Address for Server *	LDAP Port [*] Use SSL					
172.18.36.240	50000					
Add Another Redundant LDAP Server						

— Save

LDAP Filters in CUCM

The object class User is no longer used. Therefore, the LDAP filter needs to be changed to use userProxy instead of User.

The default filter is:

(&(objectclass=user)(!(objectclass=Computer))(!(msDS-UserAccountDisabled=TRUE)))

In order to modify this filter, log in to CCMAdmin with a web browser and choose the LDAP Custom Filter option from the LDAP configuration menu.

DAP Filter	Configuration
🔒 Save	
- Status	
Status:	Ready
Status: -LDAP Custor Filter Name*	Ready om Filter Information CustomFilter

This filter is used in the LDAP directory page while configuring LDAP the synchronization agreement as shown in the previous figure.

System 👻 Call Routing 👻 Media Resou	rces 👻 Advanced Features 👻 Device 👻 Application	✓ User Management ▼	Bulk Administration 👻 Help 👻					
LDAP Directory			Related Links: Back to LDAP Directory Find/L					
Save								
- I DAP Directory Information								
LDAP Configuration Name*	Multiforest							
LDAP Manager Distinguished Name st	cn=root,dc=cisco,dc=com							
LDAP Password* Confirm Password*								
		\neg						
LDAP User Search Base*	dc=cisco,dc=com							
LDAP Custom Filter	CustomFilter	~						
- LDAP Directory Synchronization	n Schedule							
Perform Sync Just Once								
Perform a Re-sync Every*	7 DAY 💌							
Next Re-sync Time (YYYY-MM-DD hh	:mm)* 2010-01-20 00:00							
Cisco Unified Communications Manag	er User Fields LDAP User Fields	Cisco Unified Commu	nications Manager User Fields LDAP User Fields					

Cisco Unified Communications Manager User Fields	LDAP User Fields	Cisco Unified Communications Manager User Fields	LDAP User Fields
User ID	mail	First Name	givenName
Middle Name	middleName 🐱	Last Name	sn
Manager ID	manager	Department	department