

Configuring Cisco Unified Communications Manager Directory Integration

Document ID: 109379

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

- Directory Integration

Configure

- Network Diagram
- Configurations
- Service Account in AD
- Directory Authentication

Troubleshooting Directory Integration (Sync)

Troubleshooting Directory Integration (Authentication)

Verify

Troubleshoot

- Error Message: Error while Connecting to ldap

Related Information

Introduction

This document provides information on how to setup, configure, and troubleshoot the Cisco Unified Communications Manager (formerly known as CallManager) Version 5.0 and later with Active Directory Integration.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of Microsoft Windows/Active Directory (AD)

Components Used

The information in this document is based on Cisco Unified Communications Manager 6.1(2)

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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Directory Integration

By default, on a non-integrated Cisco Unified Communications Manager (CUCM), there are two types of users: end users and application users.

- **End users** All users associated with a physical person and an interactive login. This category includes all IP Telephony users, as well as Unified CM administrators when you use the User Groups and Roles configuration (equivalent to the Cisco Multilevel Administration feature in prior Unified CM versions).
- **Application users** All users associated with other Cisco IP Communications features or applications, such as Cisco Attendant Console, Cisco IP Contact Center Express, or Cisco Unified Communications Manager Assistant. These applications need to authenticate with Unified CM, but these internal users do not have an interactive login. This serves purely for internal communications between applications, for example, CCMAdministrator, AC, JTAPI, RM, CCMQRTSecureSysUser, CCMQRTSysUser, CCMSysUser, IPMASecureSysUser, IPMASysUser, WDSecureSysUser, and WDSysUser.

When you integrate Cisco Unified Communications Manager with the Active Directory, the Directory Integration process uses an internal tool called Cisco Directory Synchronization (DirSync) on the Unified CM to synchronize a number of user attributes (either manually or periodically) from a corporate LDAP directory. When this feature is enabled, end users are automatically provisioned from the corporate directory.

Note: Application users are kept separate and are still provisioned through the Unified CM Administration interface. In other words, application users cannot be synchronized from AD.

In summary, end users are defined in the corporate directory and synchronized into the Unified CM database, while application users are stored only in the Unified CM database and do not need to be defined in the corporate directory.

Configure

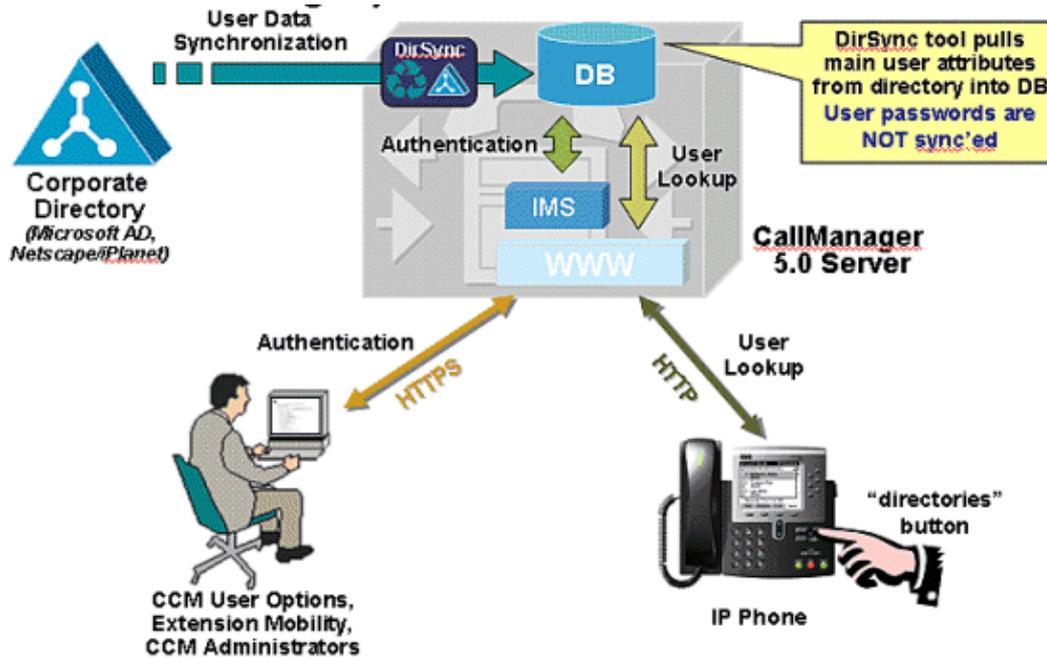
In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

Typical Directory Integration Scenario



- Active Directory: 10.48.79.37
- Domain name: Eire.com
- Cisco Unified Communications Manager : 10.48.79.93

Configurations

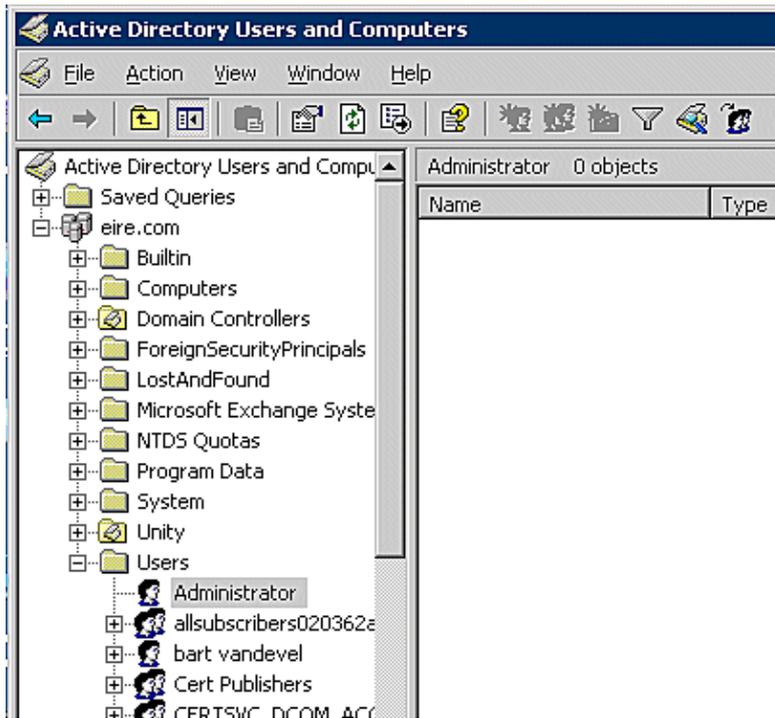
This document uses these configurations:

- Service Account in AD
- Directory Authentication
- Troubleshooting Directory Integration (Sync)
- Troubleshooting Directory Integration (Authentication)

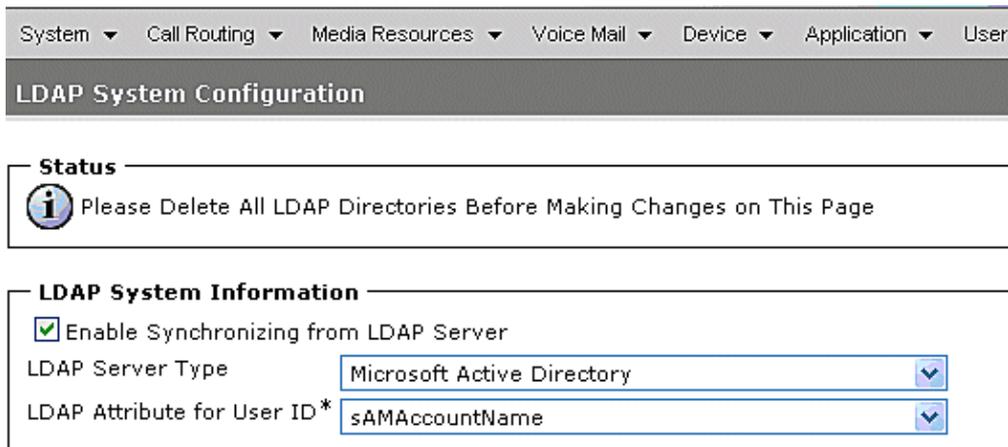
Service Account in AD

Follow these steps to create a service account in AD that allows the CM sync agreement to connect and authenticate to it.

1. This account must be able to **READ** all user objects within the desired search base and have a password set to **never expire**. In this case, the Administrator account is used, but any other account with **READ** access to all user objects within the desired search base suffices.

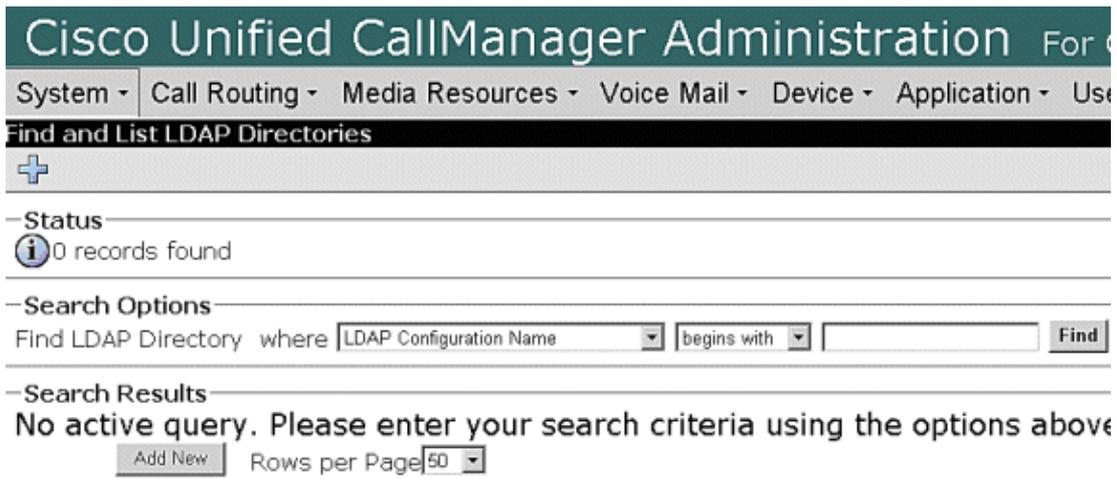


2. On Cisco Unified Communications Manager, open the ccmadmin page (<http://X.X.X.X/ccmadmin>) and navigate to **System > Ldap > Ldap System**.
3. Check the **Enable Synchronizing from LDAP Server** check box and choose **Microsoft Active Directory** for the LDAP Server Type and **sAMAccountName** for the LDAP Attribute for User ID.

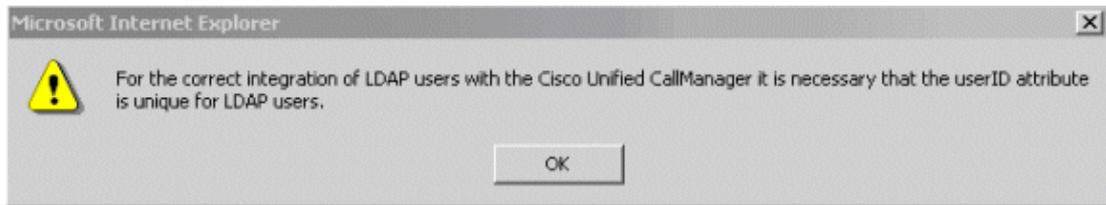


The The end users that Unified CM imports from AD are based on a standard AD attribute. In this case, **sAMAccountName** is used. Other possibilities are **Mail**, **employeeNumber**, **telephoneNumber**, or **userPrincipaName**.

4. From the CCMAdmin page, navigate to **System > Ldap > Ldap Directory** and click **Add New** to add a new Directory Replication Agreement.



5. These two windows appear, which indicate that any current user in the CM DB will be deleted once the Directory Integration is in place.



6. Fill out these fields:

- ◆ **LDAP Configuration Name:** This is any name you want to assign to the integration.
- ◆ **LDAP Manager Distinguished name:** This is the account configured in AD in Step 1. Be sure to use one of these:
 - ◇ Complete canonical name, for instance, `cn=Administrator, dc=eire, dc=com`
 - ◇ User Principal Name (UPN), for instance, `administrator@eire.com`
- ◆ **LDAP Password:** This is the password for the account configured in AD in Step 1.
- ◆ **LDAP User search base:** This path defines from where the integration pulls users from the AD.
- ◆ **LDAP Directory Synchronization Schedule.**

LDAP Directory

Save Delete Copy Perform Full Sync Now Add New

Status

Status: Ready

LDAP Directory Information

LDAP Configuration Name* Unity5

LDAP Manager Distinguished Name* administrator@eire.com

LDAP Password*

Confirm Password*

LDAP User Search Base* cn=Users, dc=eire, dc=com

LDAP Directory Synchronization Schedule

Perform Sync Just Once

Perform a Re-sync Every* 7 DAY

Next Re-sync Time (YYYY-MM-DD hh:mm)* 2008-12-11 01:54

- Define the users' fields that need to be synchronized. This defines the mapping LDAP attribute versus the attribute that the CM uses. For example, the attribute **samaccountname** maps against the attribute **userid** in the CM Informix Database. In another example, the attribute **objectguid** is mapped to the attribute **uniqueidentifier** in the CM Informix Database.
- Add the Hostname or IP for the AD server. Specify the port number (in this case 389) and check whether or not you want to use SSL.

User Fields To Be Synchronized

| Cisco Unified Communications Manager User Fields | LDAP User Fields | Cisco Unified Communications Manager User Fields | LDAP User Fields |
|--------------------------------------------------|------------------|--------------------------------------------------|------------------|
| User ID | sAMAccountName | First Name | givenName |
| Middle Name | middleName | Last Name | sn |
| Manager ID | manager | Department | department |
| Phone Number | telephoneNumber | Mail ID | mail |

LDAP Server Information

Host Name or IP Address for Server* 10.48.79.37 LDAP Port* 389 Use SSL

Add Another Redundant LDAP Server

Save Delete Copy Perform Full Sync Now Add New

- Activate and start the Cisco DirSync Service from the Serviceability page (<http://X.X.X.X/ccmservice>) **Tools > Service Activation > Cisco DirSync Tools > Control Center > Feature Services > Cisco DirSync** to finish the configuration.

Directory Services

| Service Name |
|---------------|
| Cisco DirSync |

| Status* | Activation Status |
|---------|-------------------|
| Started | Activated |

Additional service parameters that can be configured, but these can be left to default.

Service Parameter Configuration Related

Save Set to Default

Select Server and Service

Server* ▼

Service* ▼

All parameters apply only to the current server except parameters that are in the Clusterwide group(s).

Cisco DirSync (Active) Parameters on server 10.48.79.93 (Active)

| Parameter Name | Parameter Value | Suggest |
|----------------------------------------------------------------------|---------------------------------|---------|
| Clusterwide Parameters (Parameters that apply to all servers) | | |
| Maximum Number Of Agreements * | <input type="text" value="3"/> | 3 |
| Maximum Number Of Hosts * | <input type="text" value="3"/> | 3 |
| Retry Delay On Host Failure (secs) * | <input type="text" value="5"/> | 5 |
| Retry Delay On HostList Failure (mins) * | <input type="text" value="10"/> | 10 |
| LDAP Connection Timeout (secs) * | <input type="text" value="5"/> | 5 |
| Delayed Sync Start time (mins) * | <input type="text" value="5"/> | 5 |

10. You can now force a manual sync in order to synchronize the users in AD (and, more specifically, the users in the container cn=Users from the domain eire.com) to Cisco Unified Communications Manager. In order to do so, navigate to the bottom of the Directory Integration page on Cisco Unified Communications Manager (**System > Ldap > Ldap Directory**) and open the newly created Directory Integration Field. At the bottom, click the **Perform Full Sync Now** button.

— —

11. Once the sync finishes, go to the Cisco Unified Communications Manager admin pages (<http://X.X.X.X/ccmadmin>) and navigate to **User Management > Endusers**. You can now see the users that were synced from AD in the Cisco Unified Communications Manager DB with an active LDAP status.

| <input type="checkbox"/> | User ID * | First Name | Last Name | Department | LDAP Sync Status |
|--------------------------|----------------------------------|------------|-------------|------------|------------------|
| <input type="checkbox"/> | cucsvc | cucsvc | cucsvc | | Active |
| <input type="checkbox"/> | amuser | em | user | | Active |
| <input type="checkbox"/> | epasone | epas | one | | Active |
| <input type="checkbox"/> | epastwo | epas | two | | Active |
| <input type="checkbox"/> | kurt | kurt | vandevell | | Active |
| <input type="checkbox"/> | test1 | test1 | test1 | | Active |
| <input type="checkbox"/> | tim | tim | vandevell | | Active |
| <input type="checkbox"/> | unifydirsvc | unify | dirsvc | | Active |
| <input type="checkbox"/> | unifymsgstoresvc | unify | msgstoresvc | | Active |

Note: In this environment, a user had existed on Cisco Unified Communications Manager prior to running the Directory Integration.

12. After the sync, this user is now in the **Delete Pending** state.

Status
i Status: Ready

User Information
 NOTE: The add and delete function are disabled because the user directory is sync with LDAP. (i.e. The Enable Synchronization From LDAP Server flag on the LDAP System Configuration is checked).

LDAP Sync Status Delete Pending
 User ID* cmuser1
 PIN*
 Confirm PIN*
 Last name* cmuser1
 Middle name

13. Every night at 3.15 am, an internal process called the Garbage Collector service runs. This process permanently deletes any account that has been in the **Inactive Delete Pending** state for over 24 hours. The Cisco Unified Communications Manager does not sync Active Directory passwords. Cisco Unified Communications Manager has no knowledge of Microsoft Active Directory encryption mechanism. Instead, in Cisco Unified Communications Manager 5.0, a default password of **ciscocisco** and a default PIN of **12345** are assigned.

In Cisco Unified Communications Manager 6.0 and later, a default Credential Policy mechanism is used. This can be activated from the CCMAAdmin pages: **User Management > Credential Policy Default**.

Find and List Users

Status
i 14 records found

User (1 - 14 of 14) Rows per Page 50 ▾

Find User where

| Credential Policy Default | | | |
|-------------------------------------------|------------------|-----------------|--|
| Name | Credential User | Credential Type | |
| Default Credential Policy | End User | Password | |
| Default Credential Policy | Application User | Password | |
| Default Credential Policy | End User | PIN | |

14. The Credential Policy allows you to configure a default password, as well as some password policies. All users that are synchronized from AD then feed off this template for their passwords.

Credential Policy Default Configuration

 Save

Status

 Status: Ready

Credential Policy Default Information

Credential User:

Credential Type:

Credential Policy*: 

Change Credential:

Confirm Credential:

User Cannot Change

User Must Change at Next Login

Does Not Expire

15. The same applies for the PIN in Cisco Unified Communications Manager 6.0 and later.

Credential Policy Default Configuration

 Save

Status

 Status: Ready

Credential Policy Default Information

Credential User:

Credential Type:

Credential Policy*: 

Change Credential:

Confirm Credential:

User Cannot Change

User Must Change at Next Login

Does Not Expire

In other words, when Cisco Unified Communications Manager is integrated with AD (Directory Integration) but Directory Authentication has NOT been enabled (more about the Authentication mechanism later), all end users that were synchronized are authenticated locally, that is, against the Informix database in Cisco Unified Communications Manager.

Because you can authenticate locally, you can change the password of the user from Cisco Unified Communications Manager itself.

Note: This is not the case if you use Directory Authentication, as well.

User Information

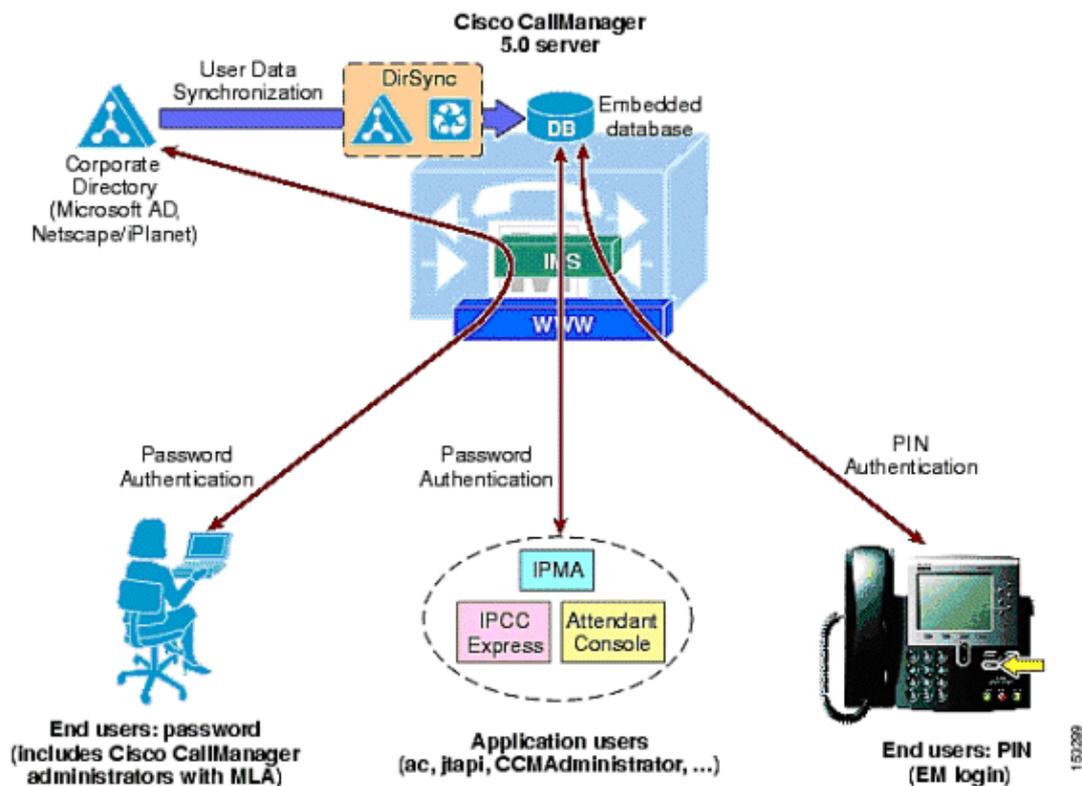
NOTE: The add and delete function are disabled because the user directory is sync with LDAP.
(i.e. The Enable Synchronization From LDAP Server flag on the LDAP System Configuration is checked).

| | | |
|------------------|---------------|------------------------------------------------|
| LDAP Sync Status | Active | |
| User ID* | kurt | |
| Password | | <input type="button" value="Edit Credential"/> |
| Confirm Password | | |
| PIN | | <input type="button" value="Edit Credential"/> |
| Confirm PIN | | |
| Last name* | vandevl | |
| Middle name | | |
| First name | kurt | |
| Telephone Number | | |
| Mail ID | kurt@eire.com | |

Directory Authentication

Directory Authentication is installed on top of Directory Synchronization, so to have Directory Authentication, Directory Integration is a prerequisite. The basic idea is the same, but the only difference is that users are authenticated against the External Directory and no longer against the Cisco Unified Communications Manager Informix database. In other words, all end user authentication attempts (for example, to access ccmuser pages, etc.) are redirected to AD.

Note: Authentication does NOT apply to application users or PINs. For instance, extension mobility PIN authentication requests are authenticated locally (against the Cisco Unified Communications Manager database) and not through AD.



1. In order to configure Directory Authentication, open the ccmadmin page (<http://X.X.X.X/ccmadmin>) and navigate to **System > Ldap > Ldap Authentication**.
2. Fill out the fields as shown in the graphic:

◆ **LDAP Manager Distinguished name:** This is the account configured in AD in Step 1. Be sure to use one of these:

◇ Complete canonical name, for instance, `cn=Administrator, dc=eire, dc=com`

◇ User Principal Name (UPN), for instance, `administrator@eire.com`

◆ **LDAP Password:** This is the password for the account configured in AD in Step 1.

◆ **LDAP User search base.**

The screenshot shows the 'LDAP Authentication' configuration page. At the top, there is a 'Save' button. Below it, the 'Status' section shows 'Status: Ready'. The 'LDAP Authentication for End Users' section has a checked checkbox 'Use LDAP Authentication for End Users'. Below this, there are four input fields: 'LDAP Manager Distinguished Name' with the value 'administrator@eire.com', 'LDAP Password' with masked characters, 'Confirm Password' with masked characters, and 'LDAP User Search Base' with the value 'cn=Users, dc=eire, dc=com'. The 'LDAP Server Information' section has a table with columns 'Host Name or IP Address for Server*', 'LDAP Port*', and 'Use SSL'. The first row contains '10.48.79.37', '389', and an unchecked checkbox. Below the table is a button labeled 'Add Another Redundant LDAP Server'.

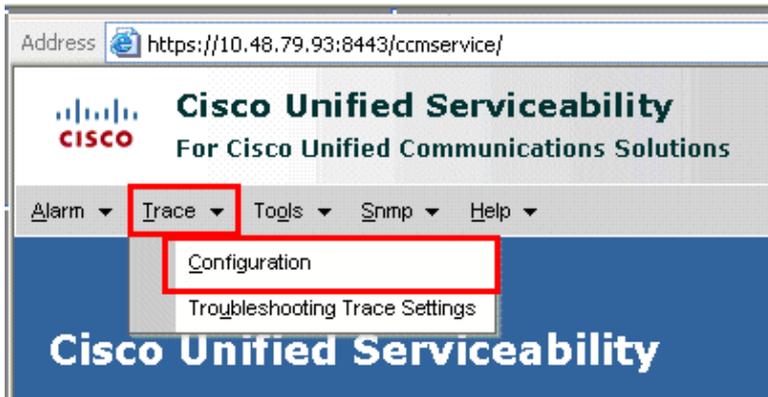
Note: When Authentication is enabled, there is no longer a password field on the configuration of individual users in Cisco Unified Communications Manager because user passwords are managed from AD and no longer from Cisco Unified Communications Manager.

The screenshot shows the 'End User Configuration' page. At the top, there is a 'Save' button. Below it, the 'Status' section shows 'Status: Ready'. The 'User Information' section has a note: 'NOTE: The add and delete function are disabled because the user directory is sync with LDAP. (i.e. The Enable Synchronization From LDAP Server flag on the LDAP System Configuration is checked)'. Below the note, there are several fields: 'LDAP Sync Status' with the value 'Active', 'User ID*' with the value 'cliff', 'PIN*' with a masked field, 'Confirm PIN*' with a masked field, 'Last name*' with the value 'richard', 'Middle name' with the value 'cliff', and 'First name' with the value 'cliff'.

Troubleshooting Directory Integration (Sync)

Scenario: You added the user Joe Bloke in AD and manually performed a sync from within Cisco Unified Communications Manager.

1. Set the `DirSync` traces to **Detailed**. Navigate to the Cisco Unified Communications Manager Serviceability page and choose **Trace > Configuration > Directory Services > DirSync**.



Trace Configuration

Select Server, Service Group and Service

Server*

Service Group*

Service*

* - indicates required item.

Trace On

Trace Filter Settings

Debug Trace Level

Cisco DirSync Trace Fields

- Enable All Trace
- Device Name Based Trace Monitoring

Include Non-device Traces

Find and List Users

15 records found

User (1 - 15 of 15)

Rows per Page 50

Find User where

| <input type="checkbox"/> | User ID ^ | First Name | Last Name | Department | LDAP Sync Status |
|--------------------------|------------------------|------------|-----------|------------|------------------|
| <input type="checkbox"/> | jbloke | Joe | Bloke | | Active |

2. In a DirSync Trace, DirSync is invoked from Cisco Unified Communications Manager:

```
2008-12-15 14:42:13,743 DEBUG [DSLdapMain] dirsync.DSLdapMain
(DSLdapMain.java:340) - DSLdapMain[handleIncomingReq] Now start
LDAPSyncImpl for agreement=f74f2069-1160-9d4a-7e8a-db6c476dd9d5
```

```
2008-12-15 14:42:13,779 INFO [DSLdapMain] ldapplugable.DSLdapSyncImpl
(DSLdapSyncImpl.java:143) - LDAPSync
(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)
[DSLdapSyncImpl] Search base=Users, dc=eire, dc=com
```

3. The account that is configured in Cisco Unified Communications Manager to fetch the users is the administrator account:

```
2008-12-15 14:42:13,787 INFO [DSLdapMain] ldapplugable.DSLdapSyncImpl
(DSLdapSyncImpl.java:147) - LDAPSync
```

```
(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)
[DSLDAPOSyncImpl] Manager DN=administrator@eire.com
Password=aa822fb730462e5bee761623f5384aef87bed6fd62280f8ec6ef01a7a4c537
```

```
2008-12-15 14:42:13,813 DEBUG [DSLDAPOMain] ldapplugable.DSLDAPOSyncImpl
(DSLDAPOSyncImpl.java:224) - LDAPSync
(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)
[DSLDAPOSyncImpl] Attributes to return - objectguid:samaccountname:
givenname:middlename:sn:manager:department:telephonenumber:mail:title:
homephone:mobile:pager:msrtcscip-primaryuseraddress:
```

```
LDAPSync(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)[makeConnection]
Successful LDAP connection to : ldap://10.48.79.37:389
```

4. Go out to AD and search for all users based on SamAccountName and objectguid within the specified user search base. Find the new user Joe Bloke:

```
LDAPSync(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)
[sendUserData] Directory entry is CN=Joe Bloke: null:null:
{mail=mail: jbloke@eire.com, objectguid=objectGUID:
[B@1ce3fc5, givenname=givenName: Joe,
samaccountname=sAMAccountName: jbloke, sn=sn: Bloke}
2008-12-15 14:42:15,351 DEBUG [DSLDAPOSyncImpl
(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)]
ldapplugable.DSLDAPOSyncImpl (DSLDAPOSyncImpl.java:926) -
LDAPSync(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)[sendUserData]
Getting ObjectGUID
```

5. Remember to fetch certain AD attributes (for example, samaccountname, objectguid, givenname, department, telephonenumber, etc.). Give them a correspondent value in the Informix DB. For example, map objectguid in AD to UniqueIdentifier within Informix on Cisco Unified Communications Manager. This is a small example of the mapping of AD to Informix. This list is only a small subset. There are several more that are not included in this document.

| CallManager DB Field | Possible AD Attributes | Possible Sun ONE Attributes |
|----------------------|----------------------------------------------------------------------------------|--------------------------------------------------|
| userid | samaccountname mail employeenumber telephonenumber userprincipalname | uid mail employeenumber telephonenumber |
| uniqueidentifier | objectguid | n/a |
| firstname | givenname | givenname |

6. In this case, map the ObjectGUID that was found for user jbloke and give a correspondent value to the UniqueIdentifier Value in Cisco Unified Communications Manager:

```
LDAPSync(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)[sendUserData]
ObjectGUID value=cc15b7817840b947990b83551140cf86
db6c476dd9d5)] ldapplugable.DSLDAPOSyncImpl (DSLDAPOSyncImpl.java:1560)
- LDAPSync(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)[formUserObject]
Name=uniqueidentifier Value=cc15b7817840b947990b83551140cf86
```

7. Next check in Informix if a user with this particular UniqueIdentifier attribute already exists:

```
2008-12-15 14:42:15,692 DEBUG [DirSync-DBInterface]
DSDBInterface.updateUserInfo Check update using uniq id.
SQL-SELECT * FROM EndUser WHERE uniqueidentifier
= 'cc15b7817840b947990b83551140cf86'
```

8. Then add the user in the Enduser table in Informix in Cisco Unified Communications Manager:

```

2008-12-15 14:42:15,724 DEBUG [DirSync-DBInterface] common.
DSDBInterface (DSDBInterface.java:377) - DSDBInterface.insert
SQL-INSERT INTO EndUser(userid,firstname,mailid,uniqueidentifier,
lastname,fkdirectorypluginconfig,status) values
('jbloke','Joe','jbloke@eire.com','cc15b7817840b947990b83551140cf86',
'Bloke','f74f2069-1160-9d4a-7e8a-db6c476dd9d5','1')

```

Troubleshooting Directory Integration (Authentication)

Scenario: You logged into the CCMUser pages with the user ID kurt Authentication redirected to AD.

1. Take a sniffer trace on Cisco Unified Communications Manager.
2. You see a Search Request.

| Frame | Time | Src MAC Addr | Dst MAC Addr | Protocol | Description | Src Other Addr | Dst Other Addr |
|-------|-----------|--------------|--------------|----------|---------------------------------------------|----------------|----------------|
| 784 | 27.402343 | 005056010106 | LOCAL | LDAP | ProtocolOp: SearchRequest (3) | 10.48.79.93 | KILKENNY |
| 785 | 27.402343 | LOCAL | 005056010106 | LDAP | ProtocolOp: SearchResponse (4) | KILKENNY | 10.48.79.93 |
| 786 | 27.417968 | 005056010106 | LOCAL | TCP | Control Bits: ...S., len: 0, seq: 72772... | 10.48.79.93 | KILKENNY |
| 787 | 27.417968 | LOCAL | 005056010106 | TCP | Control Bits: .A.S., len: 0, seq: 202521... | KILKENNY | 10.48.79.93 |


```

LDAP: ProtocolOp = SearchRequest
  LDAP: Base Object =cn=Users,dc=eire,dc=com
  LDAP: Scope = Whole subtree
  LDAP: Deref Aliases = Always Deref Aliases
  LDAP: Size Limit = No Limit
  LDAP: Time Limit = No Limit
  LDAP: Attrs Only = 0 (0x0)
  LDAP: Filter
    LDAP: Filter Type = And
      LDAP: Filter Type = And
        LDAP: Filter Type = Equality Match
          LDAP: Attribute Type =objectclass
          LDAP: Attribute Value =user
          LDAP: Filter Type = Equality Match
            LDAP: Attribute Type =sAMAccountName
            LDAP: Attribute Value =kurt
          LDAP: Attribute Description List
            LDAP: Attribute Type =distinguishedName

```

You also see a SearchResponse from AD to Cisco Unified Communications Manager for the user in question.

| Frame | Time | Src MAC Addr | Dst MAC Addr | Protocol | Description | Src Other Addr | Dst Other Addr |
|-------|-----------|--------------|--------------|----------|---------------------------------------------|----------------|----------------|
| 785 | 27.402343 | LOCAL | 005056010106 | LDAP | ProtocolOp: SearchResponse (4) | KILKENNY | 10.48.79.93 |
| 786 | 27.417968 | 005056010106 | LOCAL | TCP | Control Bits: ...S., len: 0, seq: 72772... | 10.48.79.93 | KILKENNY |
| 787 | 27.417968 | LOCAL | 005056010106 | TCP | Control Bits: .A.S., len: 0, seq: 202521... | KILKENNY | 10.48.79.93 |
| 788 | 27.417968 | 005056010106 | LOCAL | TCP | Control Bits: .A...., len: 0, seq: 72772... | 10.48.79.93 | KILKENNY |


```

TCP: Window = 63988 (0xF9F4)
TCP: Checksum = 0x4AF5
TCP: Urgent Pointer = 0 (0x0)
TCP: Options
  TCP: Option Nop = 1 (0x1)
  TCP: Option Nop = 1 (0x1)
  TCP: Timestamps Option
LDAP: ProtocolOp: SearchResponse (4)
  LDAP: MessageID = 2 (0x2)
  LDAP: ProtocolOp = SearchResponse
    LDAP: Object Name =CN=kurt vandavel,CN=Users,DC=eire,DC=com
    LDAP: Attribute Type =distinguishedName
    LDAP: Attribute Value =CN=kurt vandavel,CN=Users,DC=eire,DC=com
  LDAP: MessageID = 2 (0x2)
  LDAP: ProtocolOp = SearchResponse (simple)
    LDAP: Result Code = Success

```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Error Message: Error while Connecting to ldap

This error message appears when trying to perform LDAP integration with Cisco Unified Communications Manager:

```
Error while Connecting to ldap://10.1.1.2:636,  
javax.net.ssl.SSLException: java.lang.RuntimeException:  
Unexpected error: java.security.InvalidAlgorithmParameterException:  
the trustAnchors parameter must be non-empty
```

In order to resolve the issue, make sure that the relevant security certificate is uploaded under the CUCM OS Administration/Security/Certificate Management. Also, restart the DirSyn and Tomcat services from the Windows services.

Related Information

- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Troubleshooting Cisco IP Telephony](#) 
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 07, 2009

Document ID: 109379
