# 配置Cisco Unified通信管理器目录集成

## Contents



## Introduction

本文提供信息关于怎样用激活目录集中设置，配置和排除Cisco Unified通信管理器(以前叫作呼叫管理器)版本5.0和以上故障。

## Prerequisites

### Requirements

尝试进行此配置之前，请确保满足以下要求：

- 微软视窗/激活目录(AD)基础知识

### Components Used

本文的信息根据Cisco Unified通信管理器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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

## 背景信息

### 目录集成

默认情况下，在一个非完整的Cisco Unified通信管理器(CUCM)，有用户的两种类型：终端用户和应用程序用户。

- 终端用户—与一个物理人和一次交互式登录产生关联的所有用户。此类别包括所有IP电话用户，以及统一的CM管理员，当您使用用户组和角色配置时(等同与在前期统一的CM版本的Cisco多重管理功能)。
- 应用程序用户—所有用户与其他Cisco IP通信功能或应用程序产生关联，例如Cisco Attendant Console、Cisco IP Contact Center Express或者Cisco Unified通信管理器助理。这些应用程序需要验证与统一的CM，但是这些内部用户没有一次交互式登录。这为应用程序，例如，CCMAdministrator、AC、JTAPI、RM、CCMQRTSecureSysUser、CCMQRTSysUser、CCMSysUser， IPMASecureSysUser、IPMASysUser， WDSecureSysUser和WDSysUser之间的内部通信纯粹地服务。

当您集成Cisco Unified通信管理器与激活目录时，目录集成进程使用称为Cisco目录同步的一个内部工具(DirSync)在统一的CM同步一定数量的用户属性(手工或周期地)从一个公司LDAP目录。当此功能是启用的时，终端用户从公共目录自动地设置。

**Note:** 应用程序用户被保持分开和通过统一的CM管理界面仍然设置。换句话说，应用程序用户不可能从AD同步。

总之，而应用程序用户在统一的CM数据库在公共目录里，仅存储，并且不需要被定义终端用户在公共目录里被定义并且同步到统一的CM数据库。

## Configure

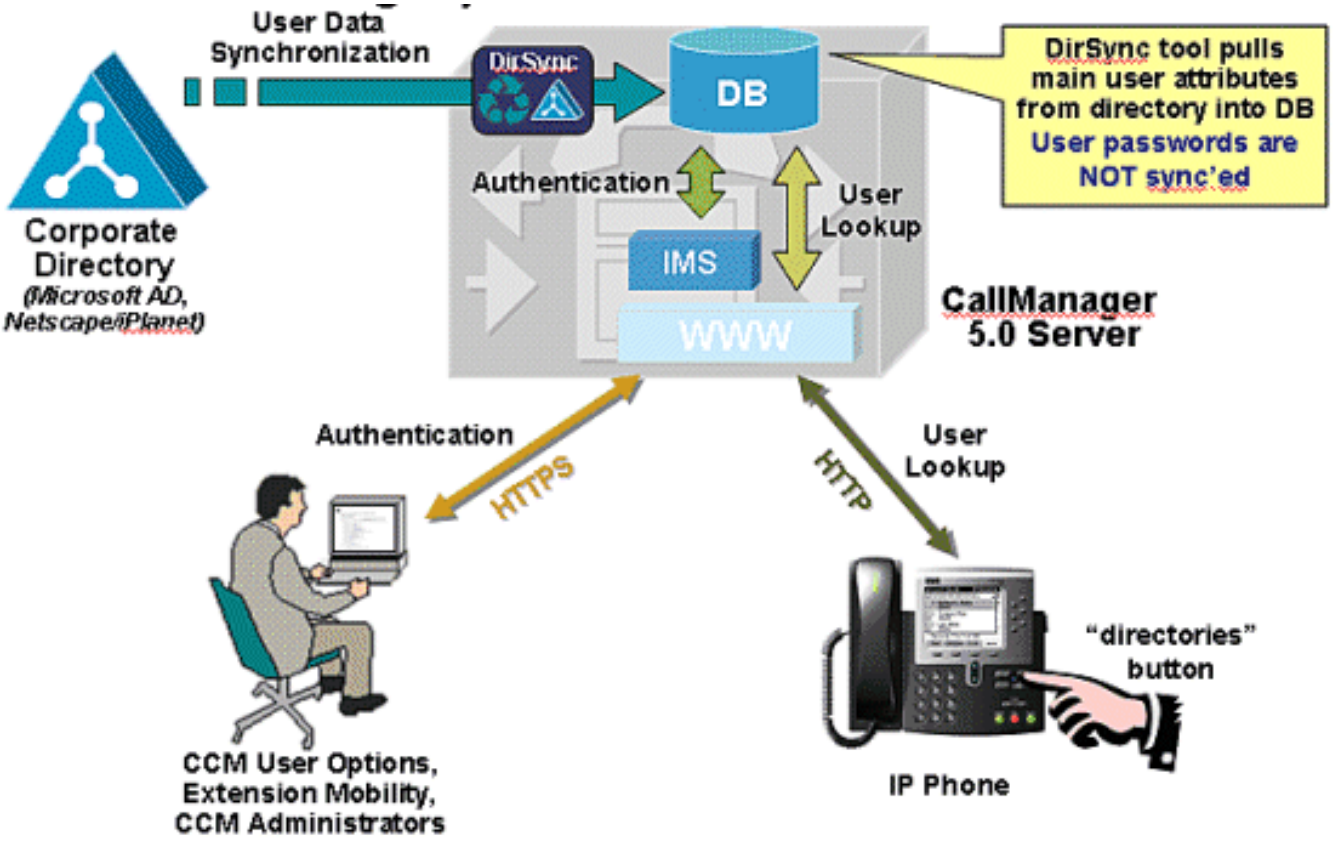
本部分提供有关如何配置本文档所述功能的信息。

**Note:** 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

### Network Diagram

本文档使用以下网络设置：

**典型的目录集成方案**




- 激活目录：10.48.79.37
- 域名：Eire.com
- Cisco Unified Communications Manager:10.48.79.93

## 配置

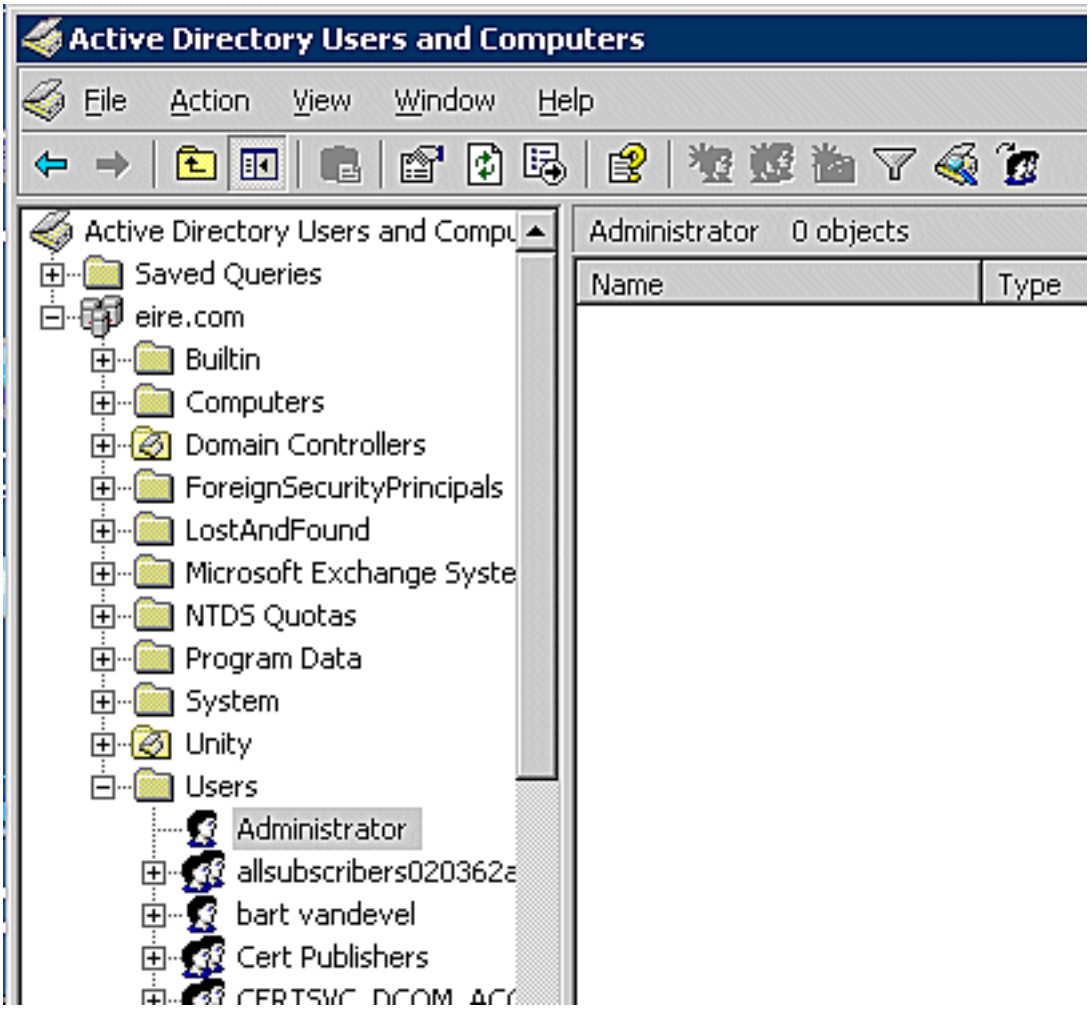
本文档使用以下配置：

- 在AD的服务帐户
- 目录认证
- 排除目录集成(同步)故障
- 排除目录集成(认证)故障

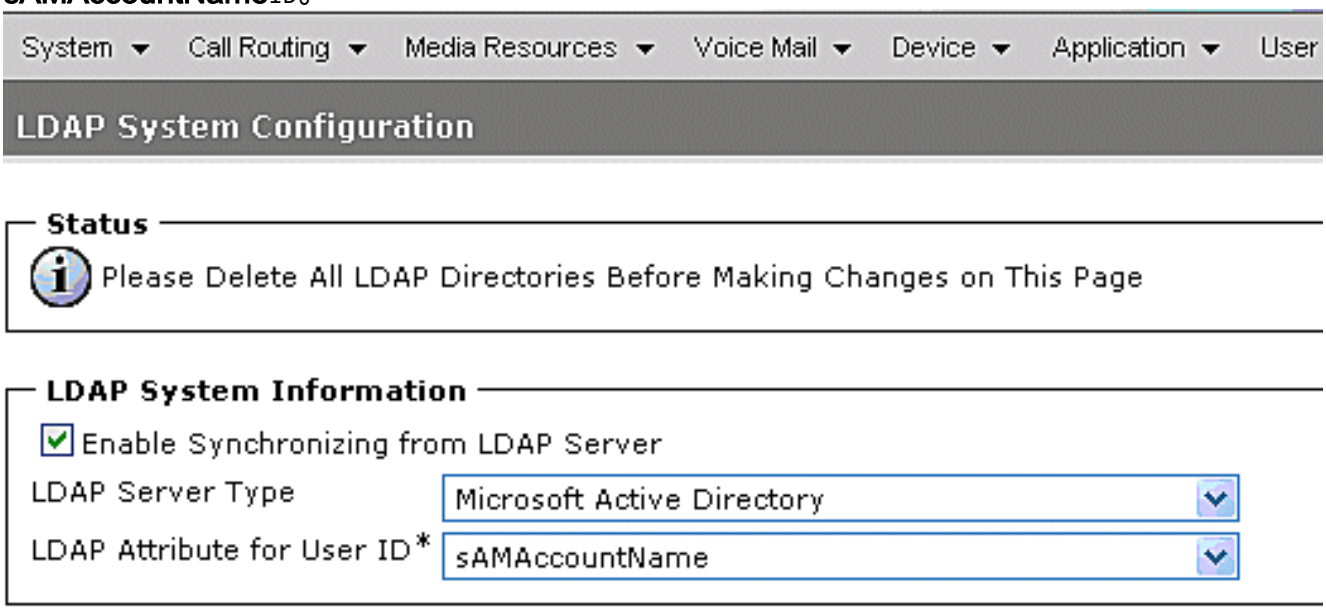
## 在AD的服务帐户

遵从这些步骤创建允许CM同步协议连接和验证到它在AD的一个服务帐户。

1. 此帐户不一定能读在期望搜索库内的所有用户对象和有**到期**的密码集合。在这种情况下，使用管理员帐户，但是与读访问的其他帐户对在期望搜索库内的所有用户对象足够了。

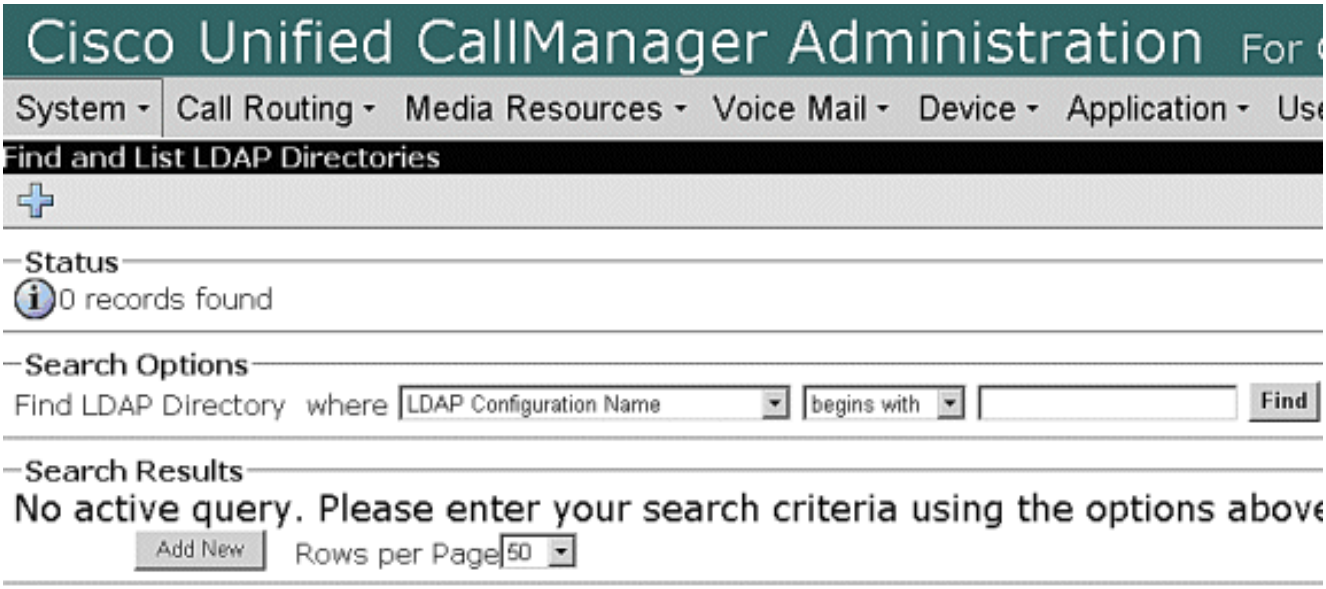



2. 在Cisco Unified通信管理器，请打开ccmadmin页(http://X.X.X.X/ccmadmin)和连接对**系统> Ldap> Ldap系统**。
3. 检查**同步从LDAP服务器**复选框的**Enable (event)**并且选择LDAPLDAP**Microsoft Active Directory**和**sAMAccountName**ID。

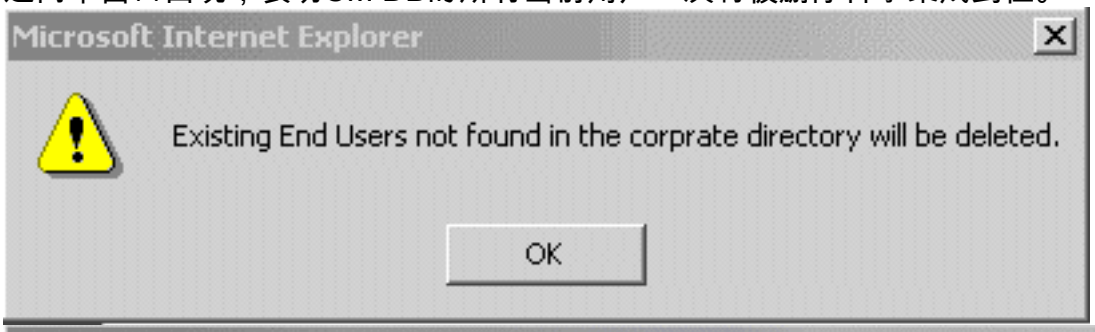


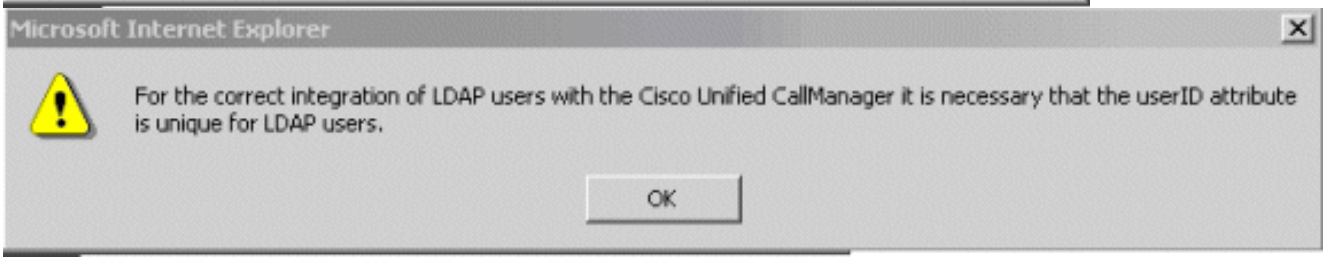

统一CM导入从AD的终端用户根据一个标准的AD属性。在这种情况下，使用**sAMAccountName**。其他可能性是**邮件、employeeNumber、telephoneNumber**或者**userPrinicpalName**。

4. 从CCMAdmin页，请连接对**系统> Ldap > Ldap目录**并且点击**添加新**添加新目录。

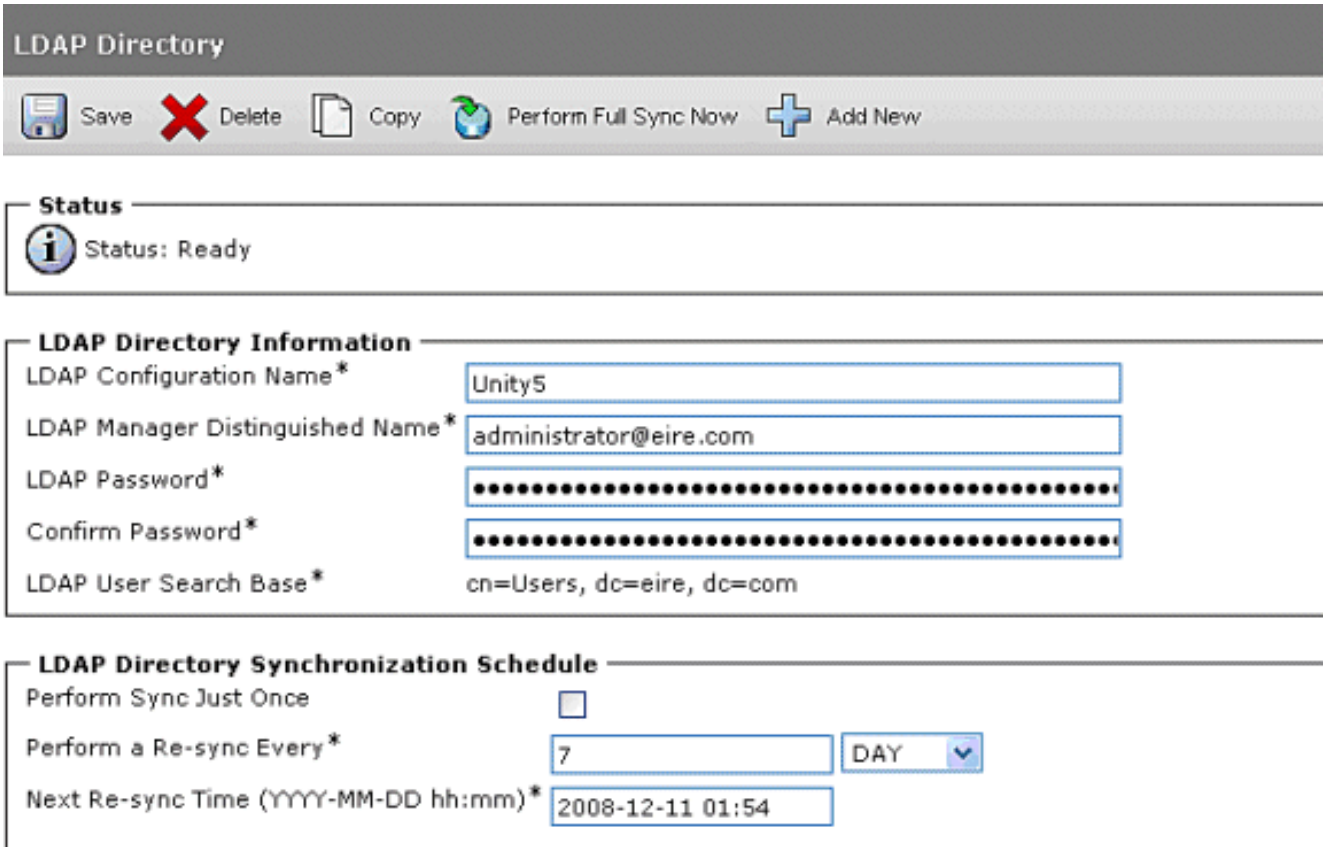



5. 这两个窗口出现，表明CM DB的所有当前用户一次将被删除目录集成到位。

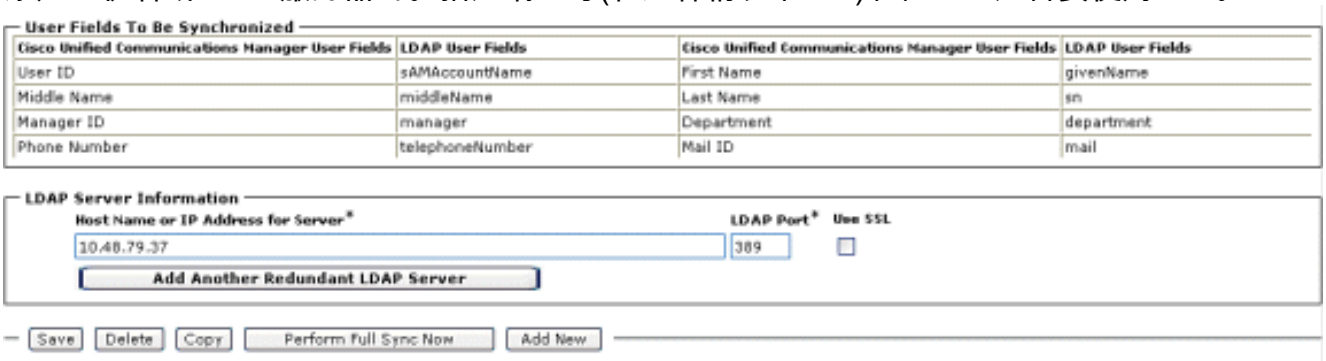


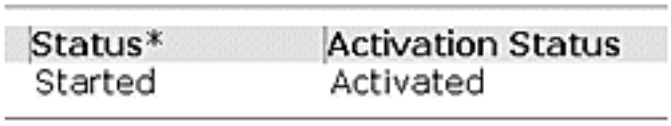

6. 填写这些字段：**IDAP配置名字**：这是您要分配到集成的所有名字。**LDAP管理器不同的名字**：这是在第1.步的AD配置的帐户是肯定使用这些中的一个：完成标准名，例如，`cn=administrator dc=eire dc=com`用户主体名字(UPN)，例如， `administrator@eire.com`**LDAP密码**：这是在Step1的AD配置的帐户的密码。**LDAP用户搜索库**：此路径从定义了集成拉从AD的地方用户。**LDAP目录同步日程表**。



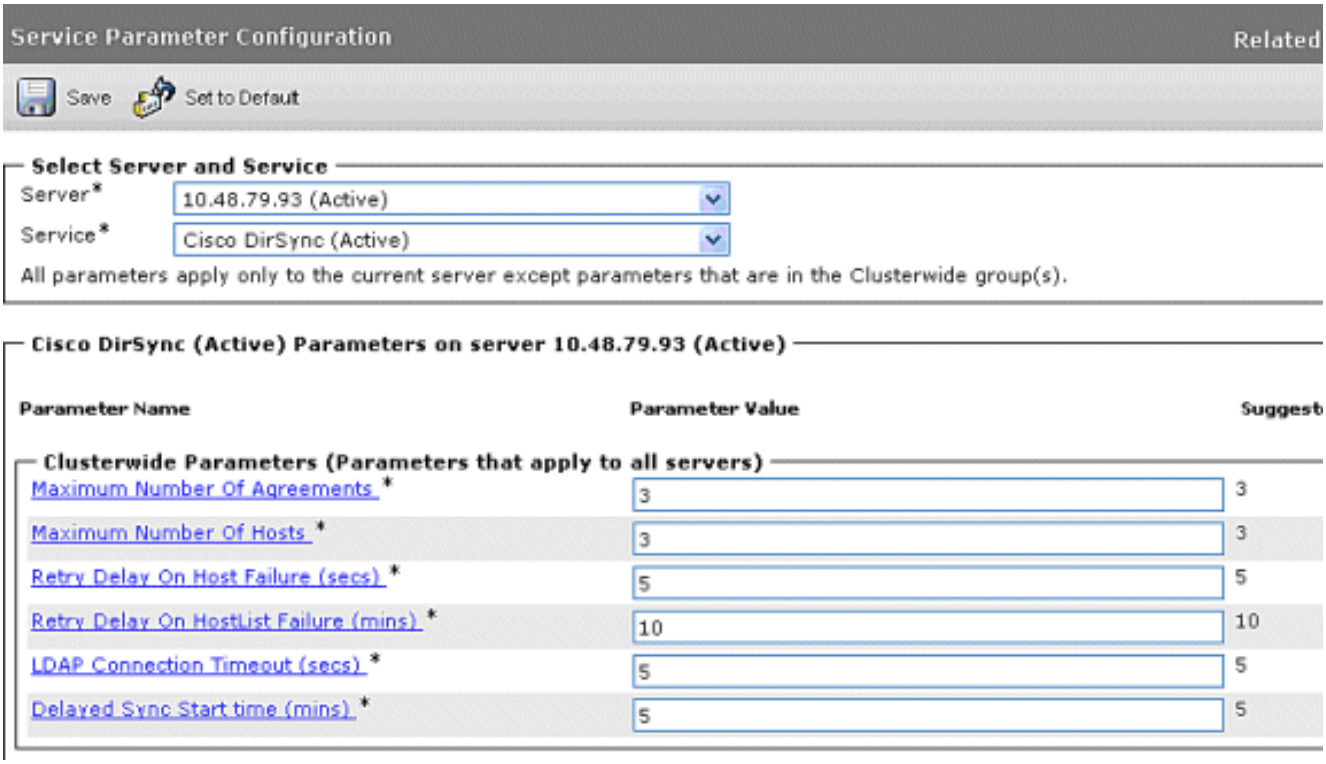

7. 定义需要同步的用户字段。这定义了映射的LDAP属性与CM使用的属性。例如，属性**samaccountname**映射在CM Informix数据库的属性**userid**。在另一个示例中，属性**objectguid**被映射对属性**uniqueidentifier**在CM Informix数据库。
8. 添加主机名或IP AD服务器的。指定端口号(在这种情况下389)和检查您是否要使用SSL。



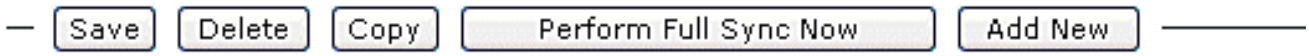

9. 启动并且开始从维护性页(http://X.X.X.X/ccmservice) **Tools > Service启动的**Cisco DirSync服务**> Cisco DirSync Tools > Control Center >功能Services>**停止配置的**Cisco DirSync**。


可以配置的其它服务参数，但是这些可以被留下默认。




10. 您能当前强制手工的同步为了同步AD的用户(并且，特别地，容器`cn=users`用户从域`eire.com`)对Cisco Unified通信管理器。为了执行如此，请连接对下面在Cisco Unified通信管理器(**系统> Ldap > Ldap目录**)的目录集成页并且打开新建立的`Integration`。在底部，**当前请**点击**执行充分的同步**按钮。

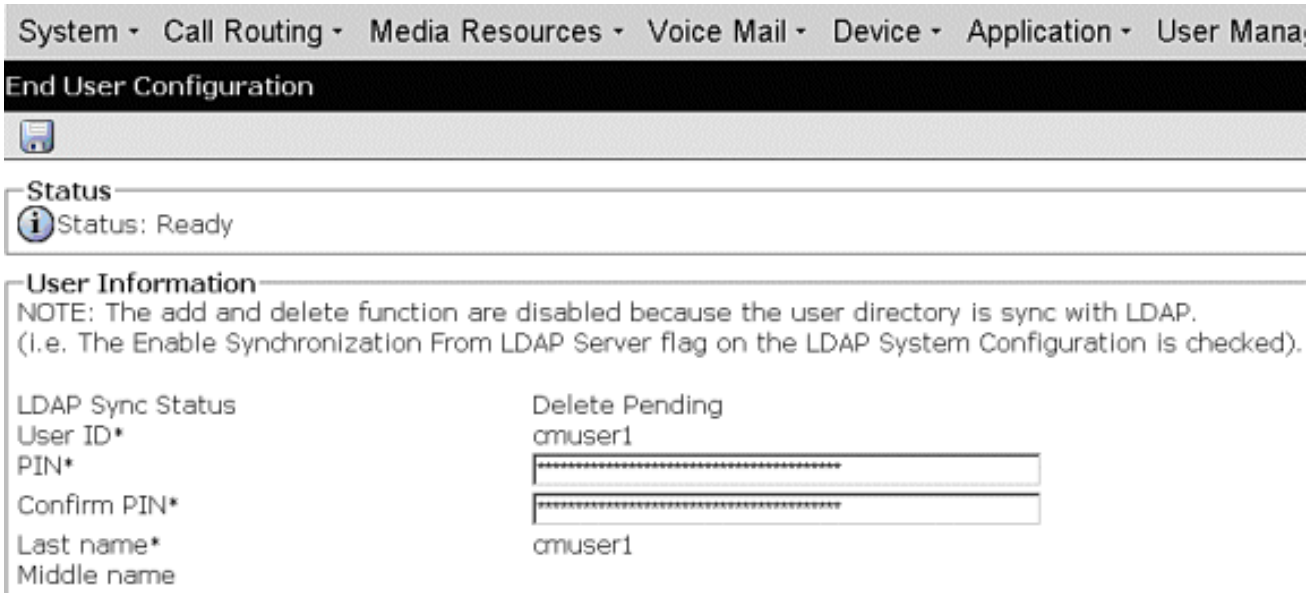



11. 一旦同步完成，请去Cisco Unified通信管理器管理员页面(`http://X.X.X.X/ccmadmin`)和连接对**用户管理>最终用户**。您能当前看到从在Cisco Unified通信管理器DB的AD同步以一个活动LDAP状态的用户。

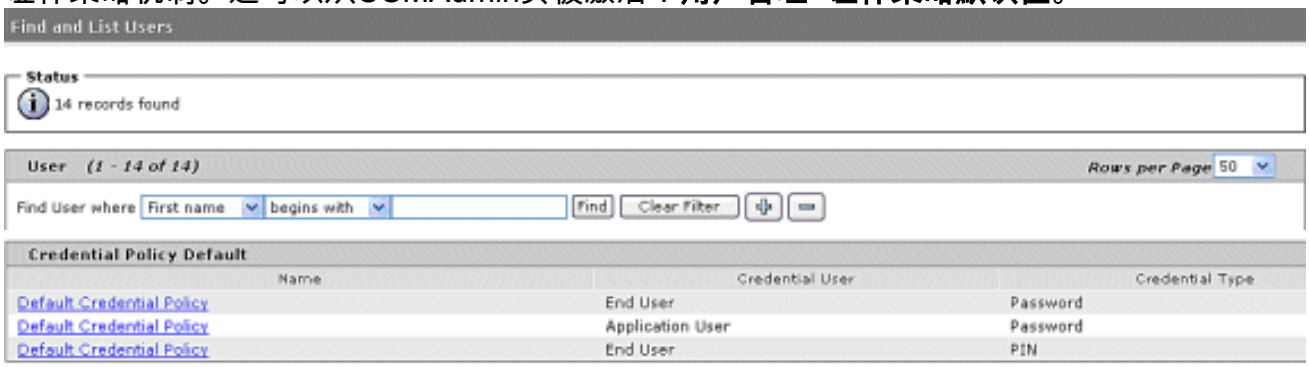
| User ID | First Name | Last Name | Department | LDAP Sync Status |
|---|---|---|---|---|
| cucsvc | cucsvc | cucsvc | | Active |
| emuser | em | user | | Active |
| epasone | epas | one | | Active |
| epastwo | epas | two | | Active |
| kurt | kurt | vandevel | | Active |
| test1 | test1 | test1 | | Active |
| tim | tim | vandevel | | Active |
| unitydirsvc | unity | dirsvc | | Active |
| unitymsgstoresvc | unity | msgstoresvc | | Active |

**Note:** 在此环境里，用户在Cisco Unified通信管理器存在了在运行目录集成之前。

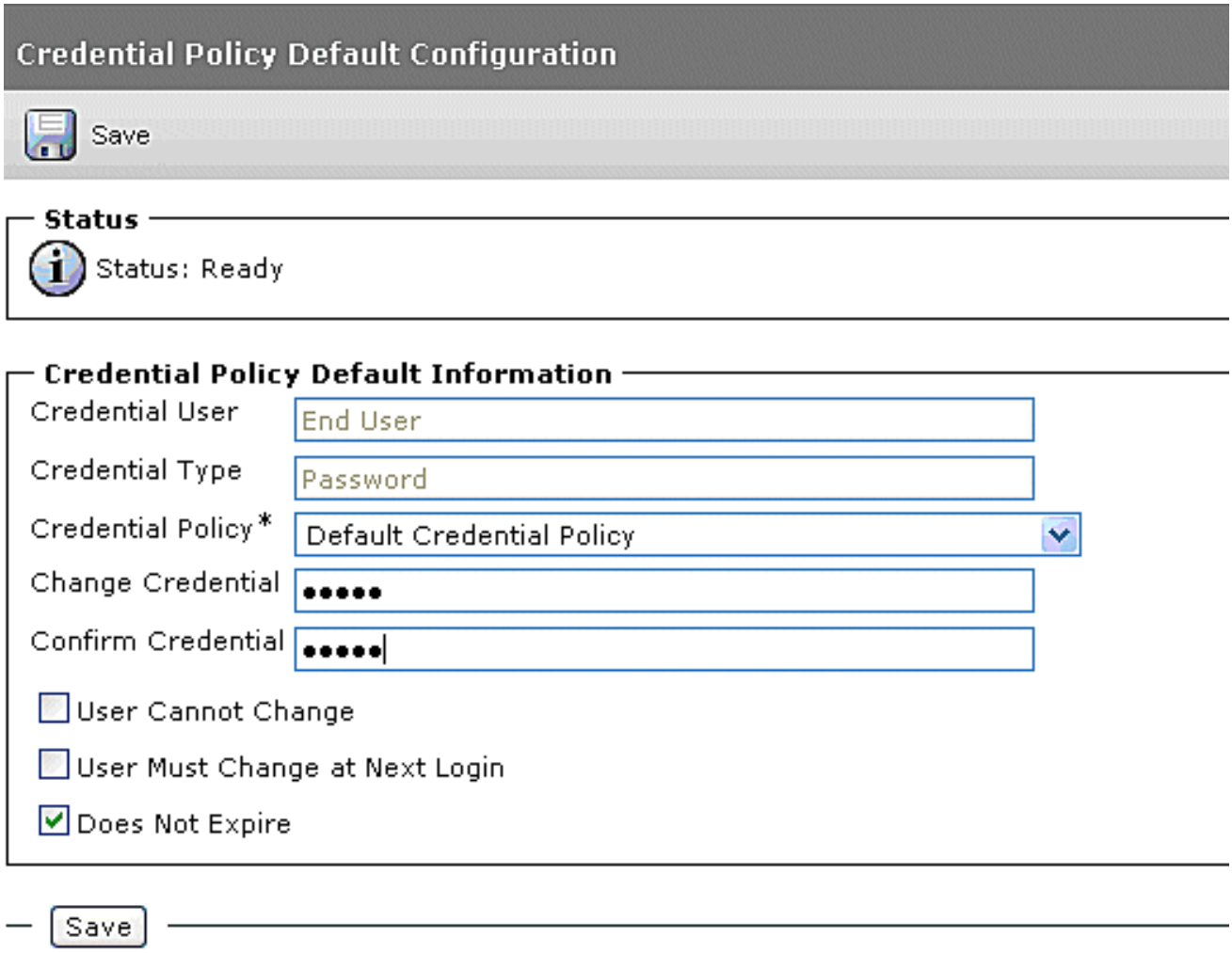
12. 在同步，此用户当前在**删除待定**状态后。



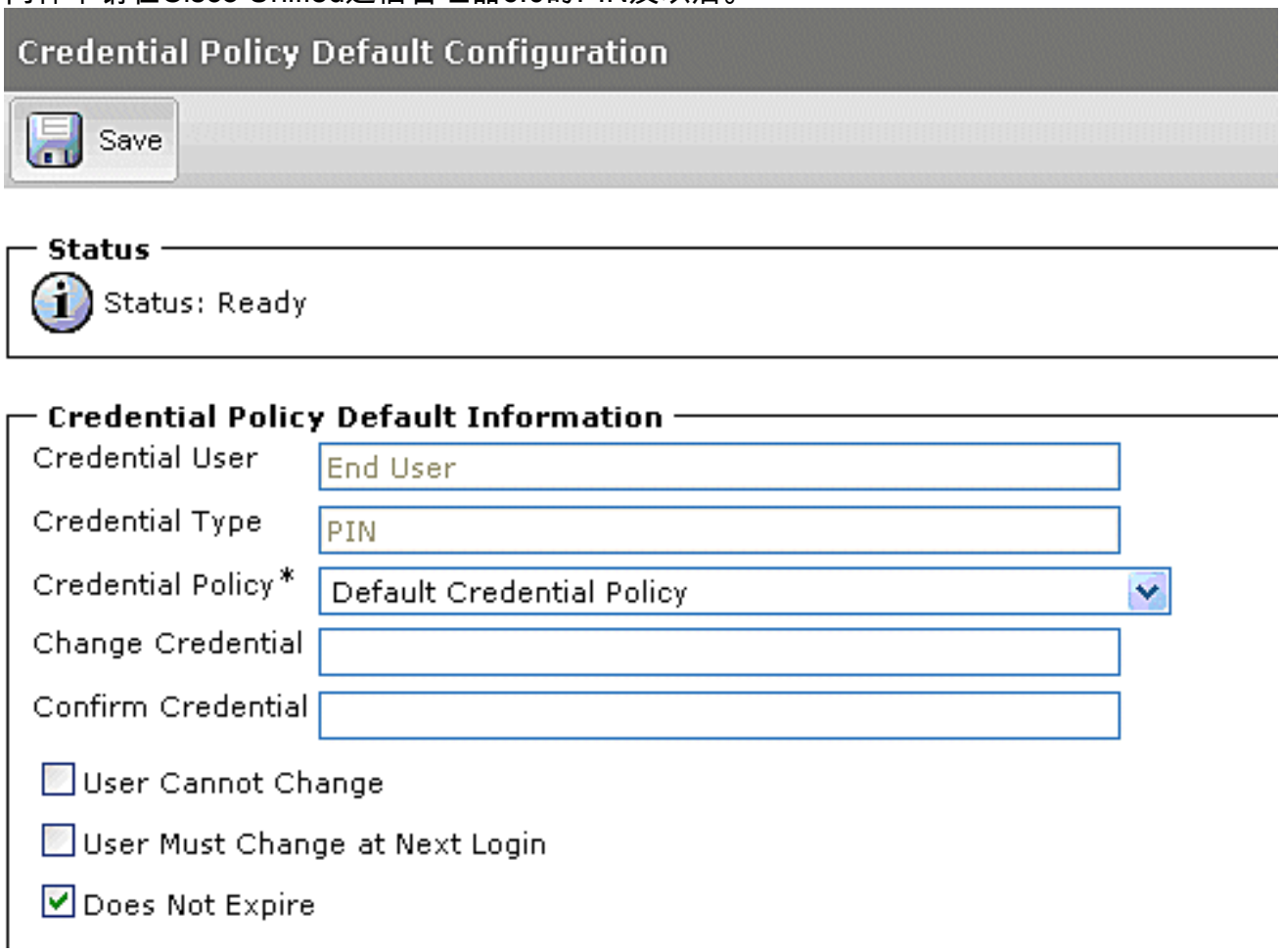

13. 每晚在3.15上午，一个内部进程呼叫碎片收集器服务运行。此进程永久删除在**非激活的**所有帐户**–删除等待**状态24小时。Cisco Unified通信管理器不同步激活目录密码。Cisco Unified通信管理器不了解Microsoft Active Directory加密机制。反而，在Cisco Unified通信管理器5.0，**ciscocisco**默认密码和默认PIN **12345**分配。在Cisco Unified通信管理器6.0及以后，使用默认证件策略机制。这可以从CCMAdmin页被激活：**用户管理>证件策略默认值**。




14. 允许您配置默认密码，以及一些密码策略。从AD同步然后的所有用户提供他们的密码的此模板。

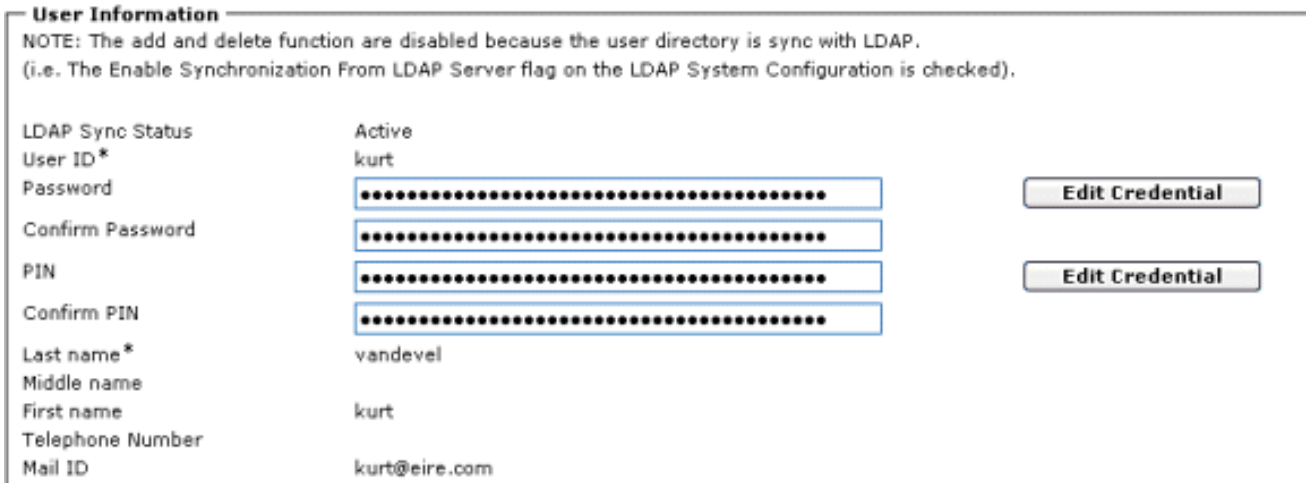



15. 同样申请在Cisco Unified通信管理器6.0的PIN及以后。



换句话说，当Cisco Unified通信管理器集成AD (目录集成)时，但是目录认证未被启用(更多关于后认证机制)，同步的所有终端用户本地验证，即，在Cisco Unified通信管理器的Informix数据库。由于您能本地验证，您能从Cisco Unified通信管理器更改用户的密码。

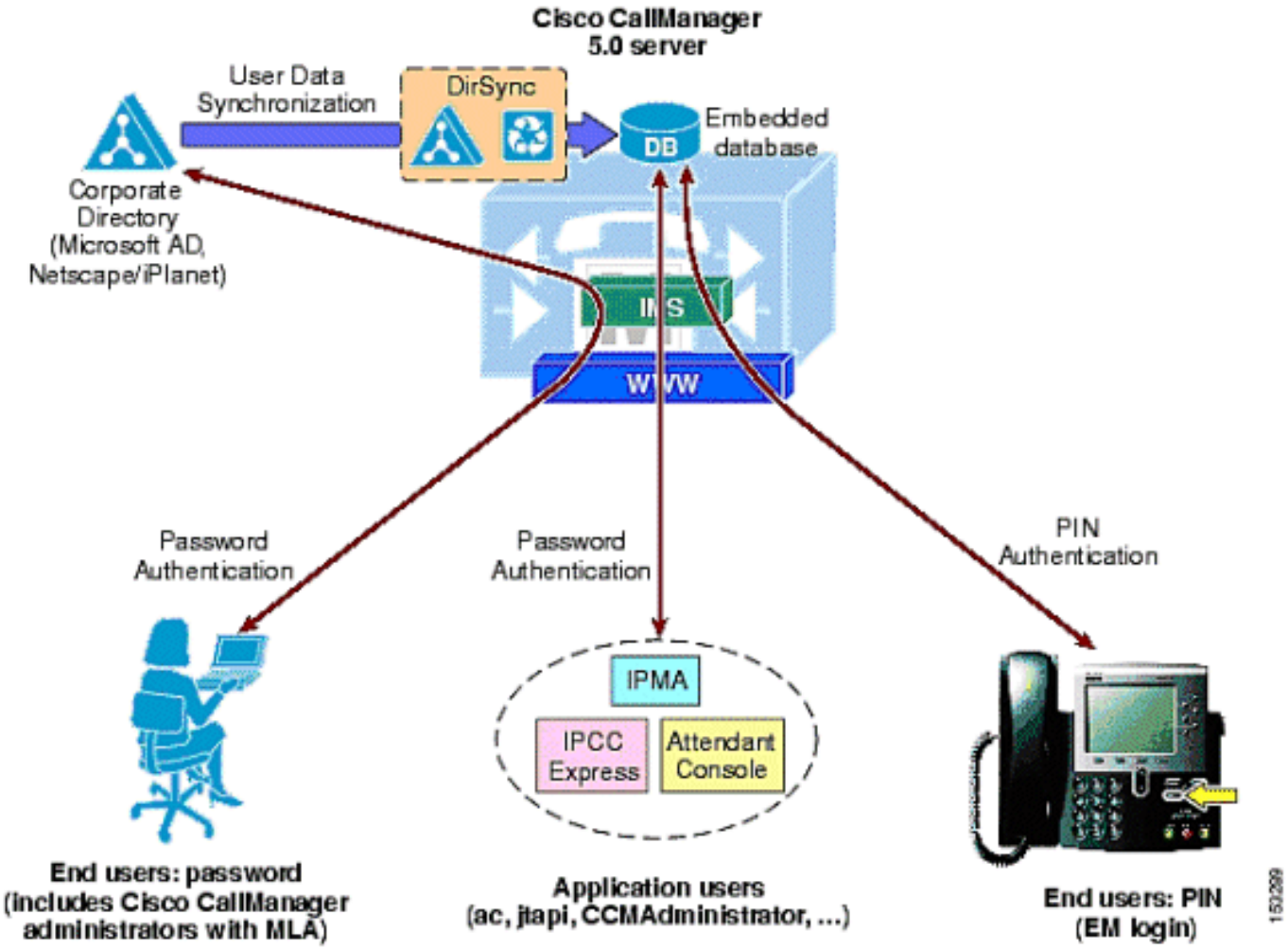
**Note:** 这不是实际情形，如果使用目录认证。



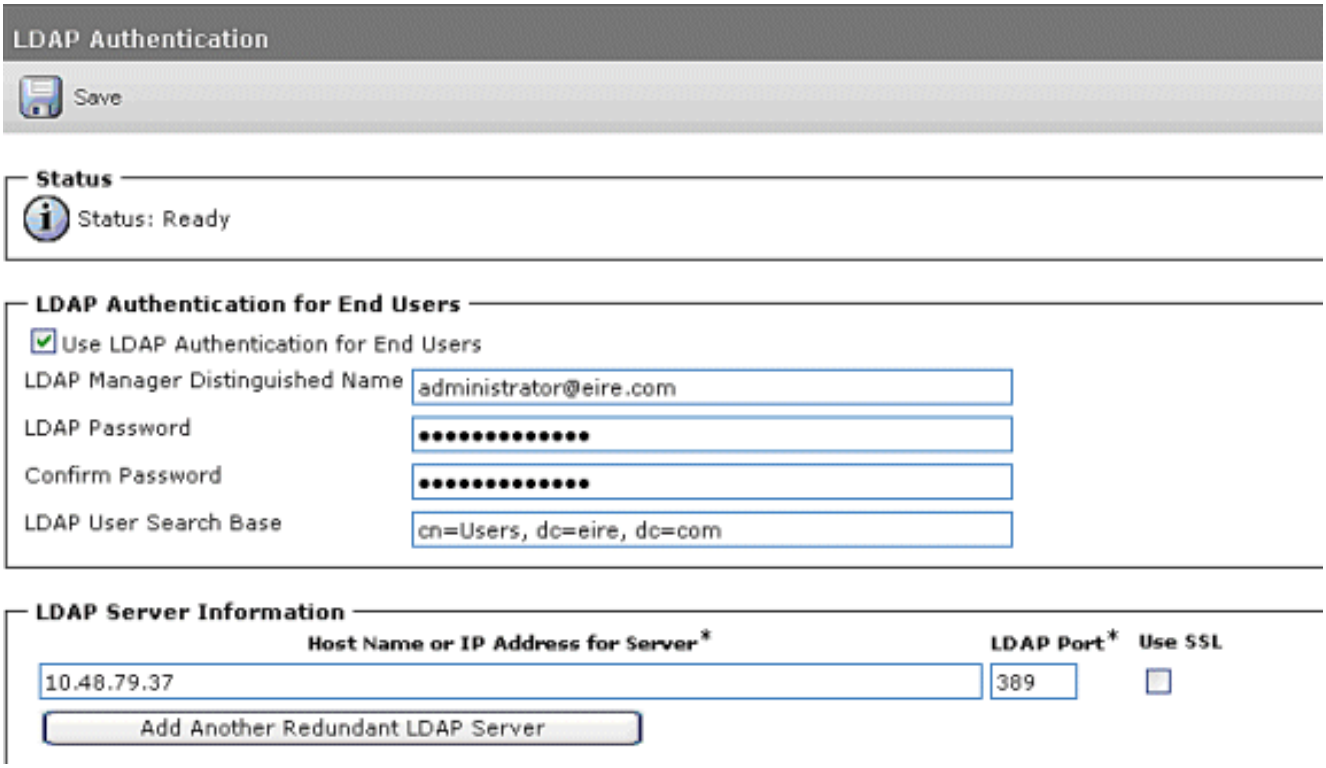

## 目录认证

目录认证安装在目录同步顶部，因此有目录认证，目录集成是前提。基本想法是相同的，但是唯一的区别是用户验证外部目录和不再利用Cisco Unified通信管理器Informix数据库。换句话说，所有终端用户认证尝试(例如，访问ccmuser页等等)重定向对AD。

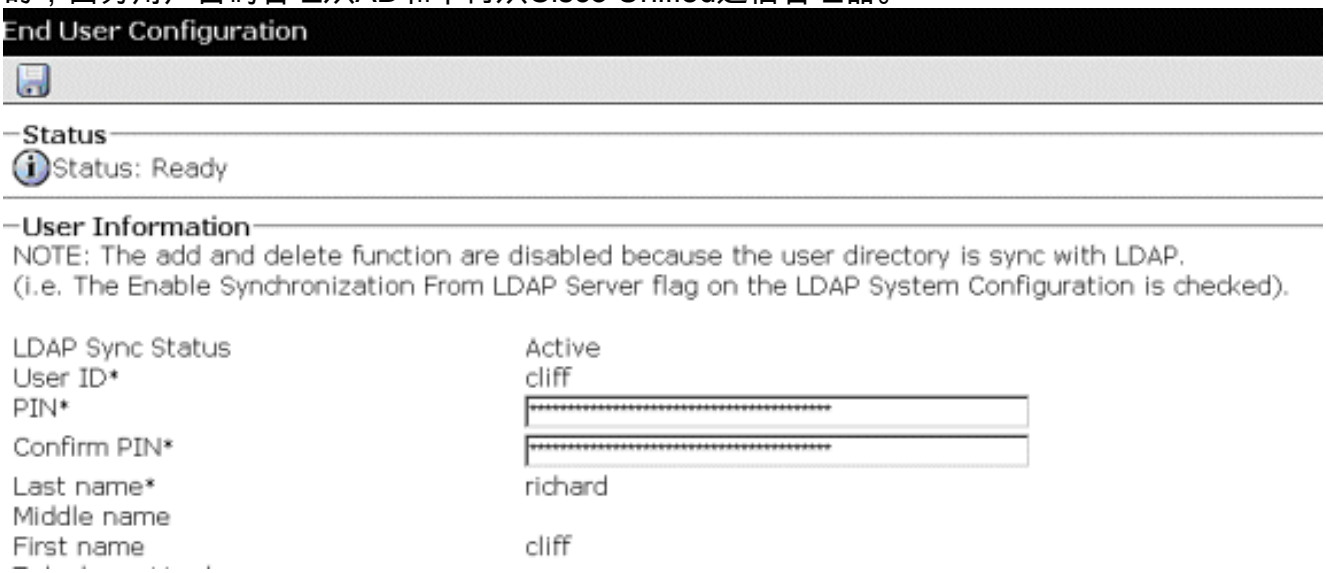
**Note:** 认证不适用于应用程序用户或管脚。例如，扩展移动性PIN认证请求本地验证(Cisco Unified通信管理器数据库)和不通过AD。




1. 为了配置目录认证，请打开ccmadmin页(http://X.X.X.X/ccmadmin)和连接对**系统> Ldap > LDAP认证。**
2. 如图形所显示，填写字段：**LDAP管理器不同的名字**：这是在第1.步的AD配置的帐户是肯定使用这些中的一个：完成标准名，例如， `cn=administrator dc=eire dc=com`用户主体名字(UPN)，例如， `administrator@eire.com`**LDAP密码**：这是在Step1的AD配置的帐户的密码。**LDAP用户搜索库。**



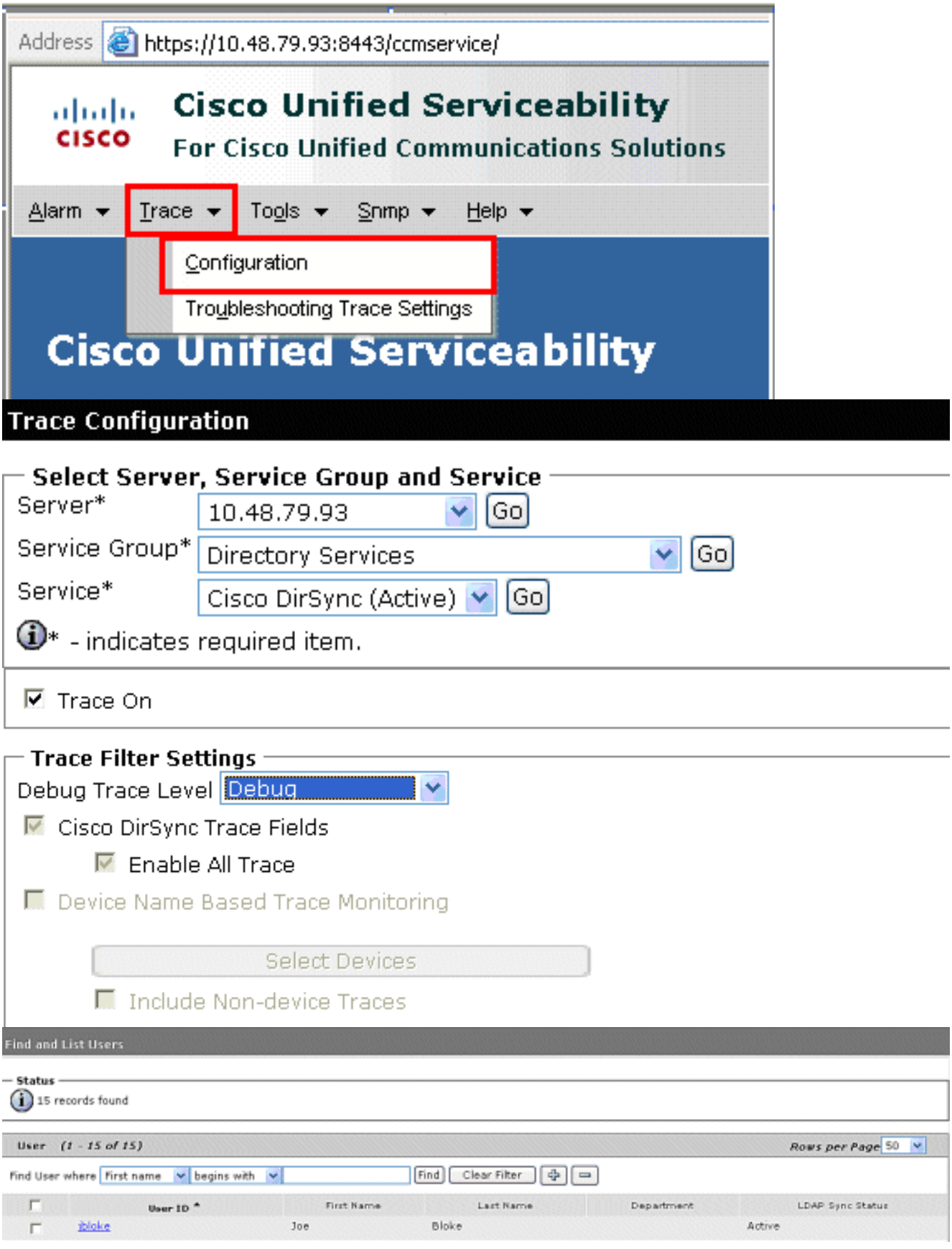

**Note:** 当认证是启用的时，不再有在个人用户的配置的一个密码字段Cisco Unified通信管理器的，因为用户密码管理从AD和不再从Cisco Unified通信管理器。




## 排除目录集成(同步)故障

**方案：**您添加了AD的用户Joe男人和手工执行同步从Cisco Unified通信管理器的内部。

1. 设置`DirSync`对**详细**。连接对Cisco Unified通信管理器维护性页并且选择**Trace > Configuration >目录Services> DirSync**。




2. 在DirSync跟踪， DirSync从Cisco Unified通信管理器被调用：

```
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=cn=Users, dc=eire, dc=com
```

3. 在Cisco Unified通信管理器被配置拿来用户的帐户是管理员帐户：

```
2008-12-15 14:42:13,787 INFO  [DSLDAPMain] ldapplugable.DSLDAPSyncImpl
   (DSLDAPSyncImpl.java:147) - LDAPSync
   (f74f2069-1160-9d4a-7e8a-db6c476dd9d5)
   [DSLDAPSyncImpl] Manager DN=administrator@eire.com
Password=aa822fb730462e5bee761623f5384aef87bed6fd62280f8ec6ef01a7a4c537

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

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

4. 出去对AD并且搜索根据SamAccountName和objectguid的所有用户在指定的用户搜索库内。寻找新用户Joe男人：

```
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 [DSLDAPSyncImpl
   (f74f2069-1160-9d4a-7e8a-db6c476dd9d5)]
   ldapplugable.DSLDAPSyncImpl (DSLDAPSyncImpl.java:926) -
   LDAPSync(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)[sendUserData]
   Getting ObjectGUID
```

5. 切记拿来某些AD属性(例如， samaccountname、objectguid、givenname、、telephonenumber等等)。产生他们在Informix公司DB的对应的值。例如，请映射“objectguid”在AD对“UniqueIdentifier”在Cisco Unified通信管理器的Informix公司内。这是AD映射的一个小的示例对Informix公司。此列表是仅小的子集。有在本文没有包括的几更多。

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

6. 在这种情况下，请映射为用户jbloke被找到的ObjectGuid并且产生对应的值在Cisco Unified通信管理器的UniqueIdentifier值：

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

```
- LDAPSync(f74f2069-1160-9d4a-7e8a-db6c476dd9d5)[formUserObject]
Name=uniqueidentifier Value=cc15b7817840b947990b83551140cf86
```

7. 如果有此特定的UniqueIdentifier属性的一个用户已经存在，下请登记Informix公司：

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

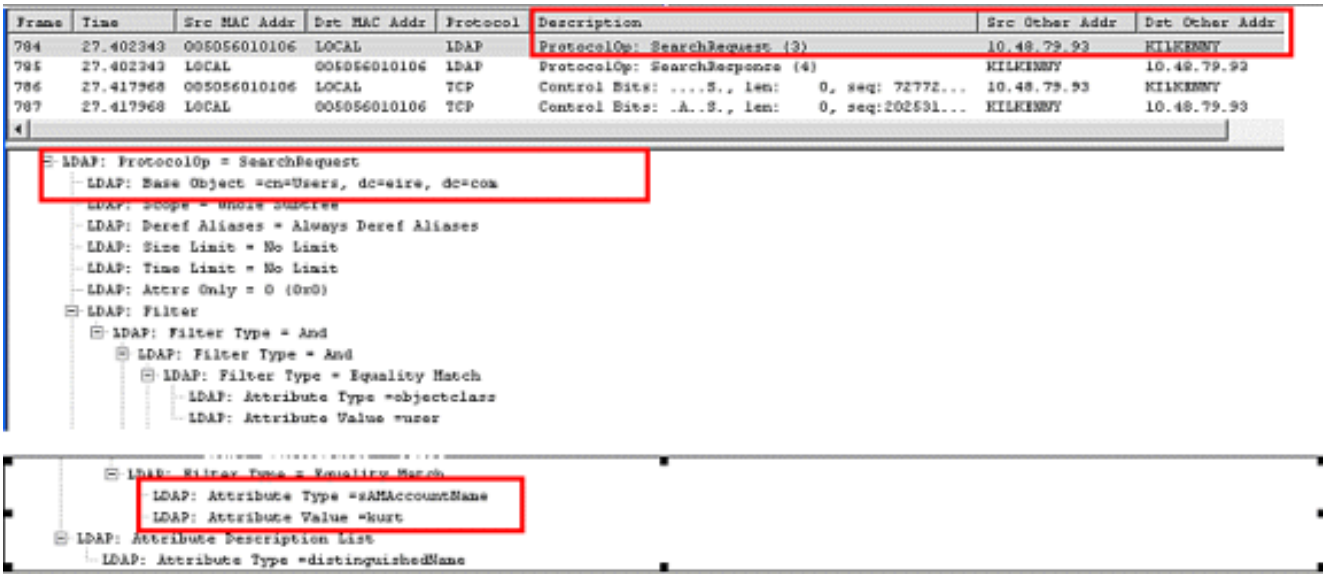
8. 然后请添加用户在最终用户表里在Cisco Unified通信管理器的Informix公司中：

```
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')
```

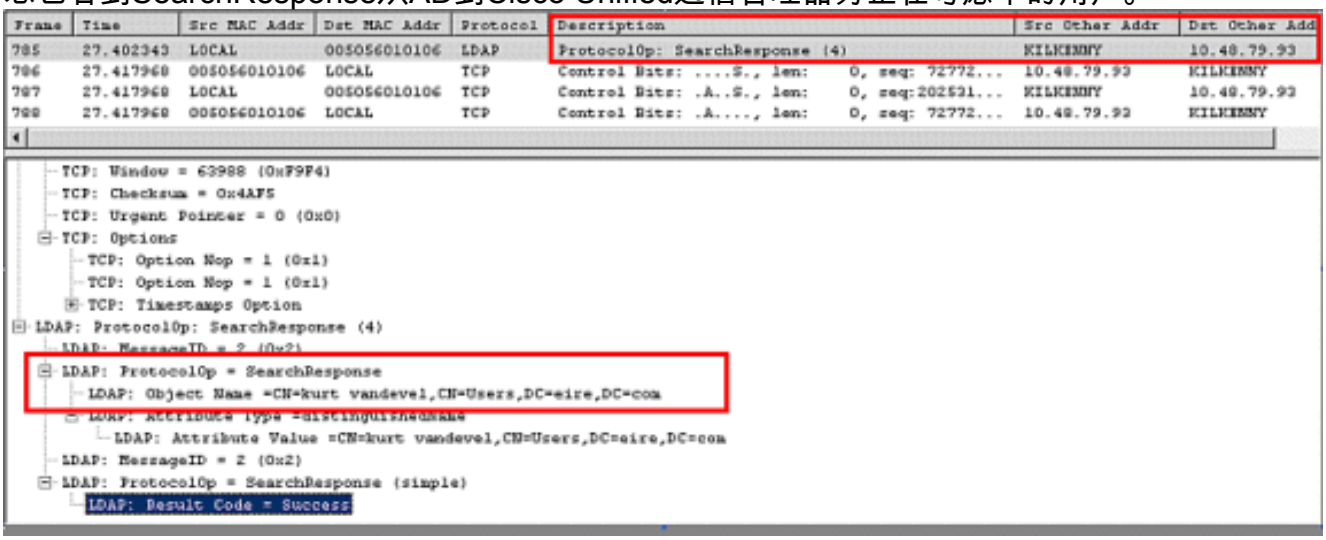
## 排除目录集成(认证)故障

**方案**：您记录了到Ccmuser与用户ID “寇特”认证的页重定向对AD。

1. 采取在Cisco Unified通信管理器的嗅探器跟踪。
2. 您看到搜索请求。




您也看到SearchResponse从AD到Cisco Unified通信管理器为正在考虑中的用户。



# Verify

当前没有可用于此配置的验证过程。

# Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

## 错误消息：错误，当连接到ldap时

此错误信息出现，当设法进行LDAP集成与Cisco Unified通信管理器时：

```
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')
```

为了解决问题，请切记相关安全证书被加载在CUCM OS管理/安全/证书管理下。并且，请重新启动从Windows服务的DirSyn和Tomcat服务。

# Related Information

- 语音技术支持
- 语音和统一通信产品支持
- Cisco IP 电话故障排除
- Technical Support & Documentation - Cisco Systems