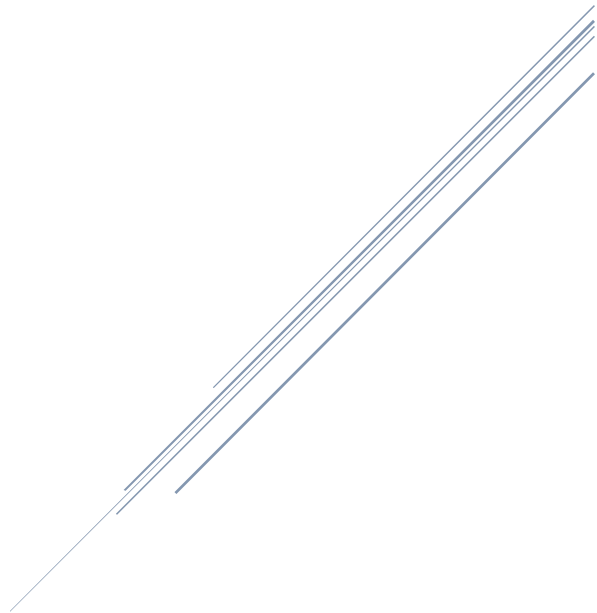


# CONFIGURACION CISCO CALL MANAGER Y JABBER



## Versiones de los Servidores

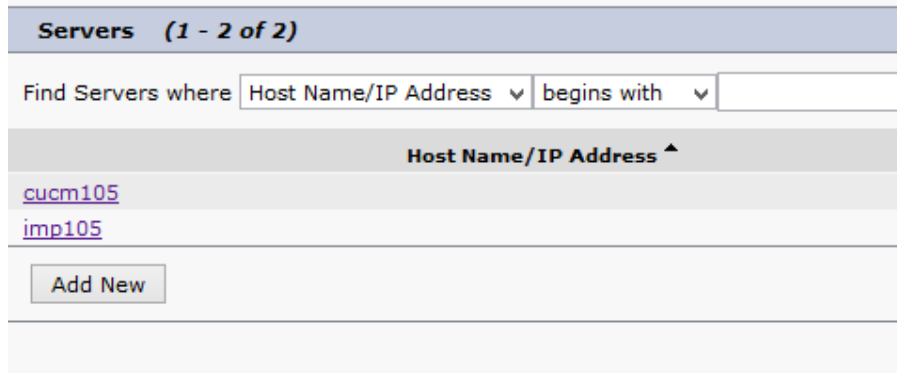
Cisco Unified Communication Manager	10.5.1.10000-7
Cisco Unified IM & Presence	10.5.1.10000-9
Microsoft Windows Server 2012	

## Direccionamiento

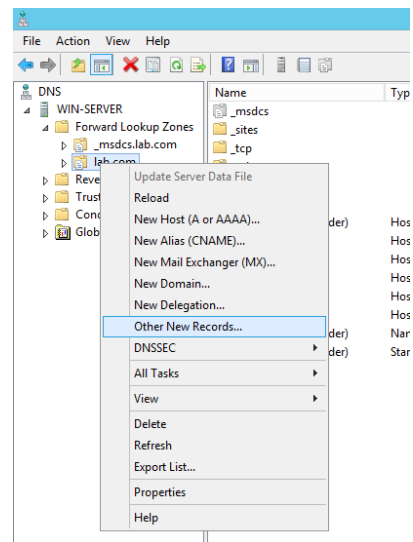
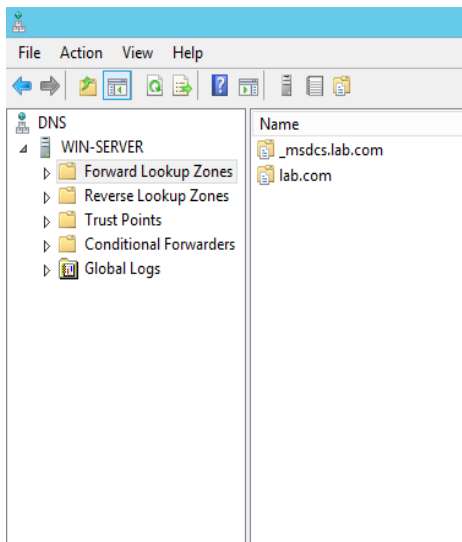
Servidor	Host name	User	Password	IP Address
DNS/Active Directory	WIN-SERVER	Administrator	C1sc0#123	10.10.10.10 /24
CUCM 10.5	cumc105	Platform/Administrator	C1sc0#123	10.10.10.100 /24
		system security Password	C1sc0#123	
		Application/Administrator	C1sc0#123	
IM&Presence 10.5	imp105	Administrator	C1sc0#123	10.10.10.101 /24

## Configuración DNS Service Records

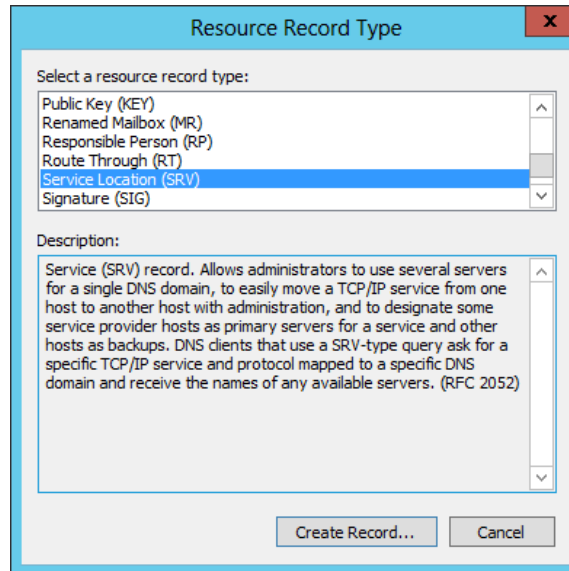
En el Callmanager modificamos las ips de nuestros servidores y ponemos el hostname  
Para eso nos vamos a **System > Server** y cambiamos la IP por hostname



Abrimos el Servidor de DNS, en nuestro árbol de dominio buscamos **Forward Lookup Zone > (dominio.com)**.  
Hacemos click derecho y seleccionamos **Other New Records**

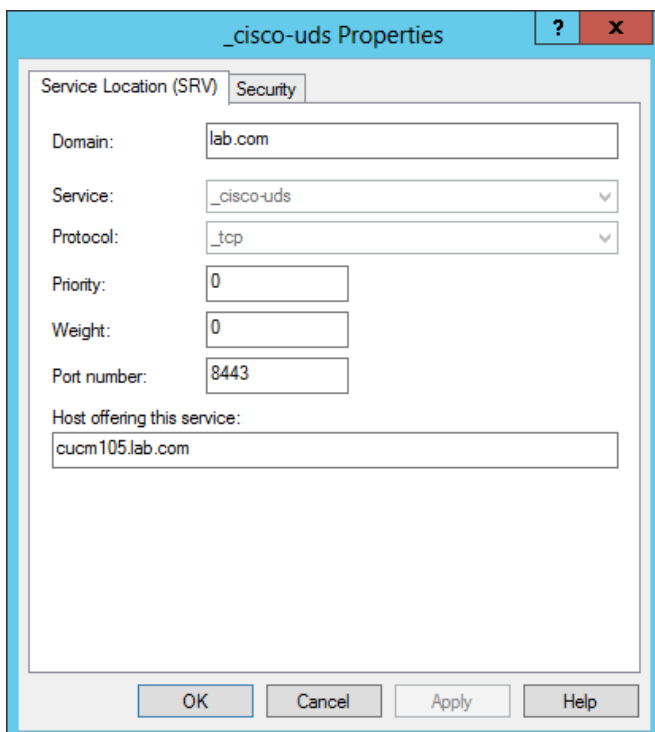


En la ventana que nos aparece buscamos **Service Location (SRV)** y **Create Record**



Llenamos los campos de la siguiente manera:

- **Domain** .- se completa automáticamente con nuestro dominio
- **Service** .- **\_cisco-uds**
- **Protocol** .- **\_tcp**
- **Priority** .- **0 ( por default )**
- **Weight** .- **0 ( por default )**
- **Port Number** .- **8443**
- **Host Offering This Service** .- **cucm105.lab.com** ( es el hostname de nuestro Call Manager -FQDN )

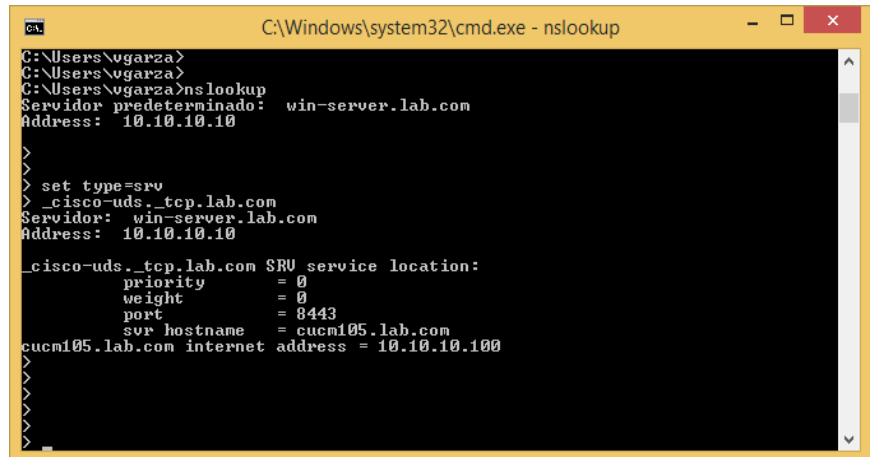


Para verificar esta configuración de DNS , en una PC dentro del dominio abrimos una ventana de comandos cmd

Escribimos: **nslookup**,

Escribimos: **set type=srv**

Escribimos: **\_cisco-uds.\_tcp.lab.com**  
**(nuestro dominio)**



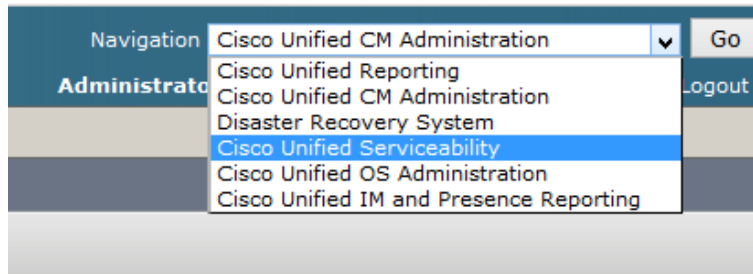
```
C:\Windows\system32\cmd.exe - nslookup
C:\Users\ogarza>
C:\Users\ogarza>
C:\Users\ogarza>nslookup
Servidor predeterminado: win-server.lab.com
Address: 10.10.10.10
>
> set type=srv
> _cisco-uds._tcp.lab.com
Servidor: win-server.lab.com
Address: 10.10.10.10

_cisco-uds._tcp.lab.com SRV service location:
    priority = 0
    weight = 0
    port = 8443
    svr hostname = cucm105.lab.com
cucm105.lab.com internet address = 10.10.10.100
>
>
>
```

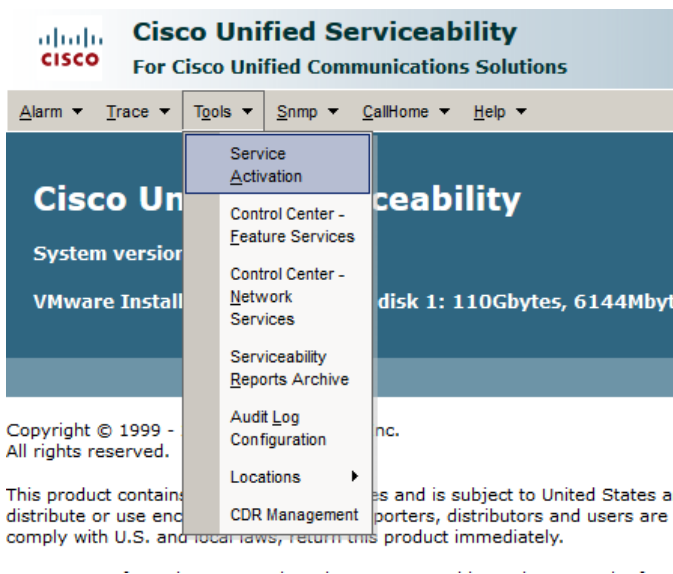
Si nos aparece los que configuramos anteriormente quiere decir que lo hicimos bien.

## Activar los servicios de Call Manager y Presence

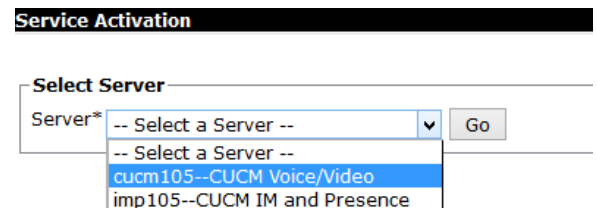
Nos loguemos en nuestro call manager y nos vamos a **Cisco Unified Serviceability** para activar los servicios...



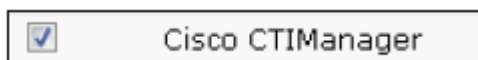
Seleccionamos **Tools > Service Activation** en el menú.



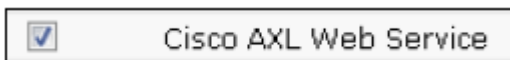
Seleccionamos nuestro call manager.



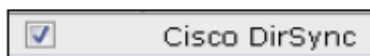
Activamos estos servicios y hacemos click en **Save**:



Este servicio es necesario para ejecutar desk phone control.



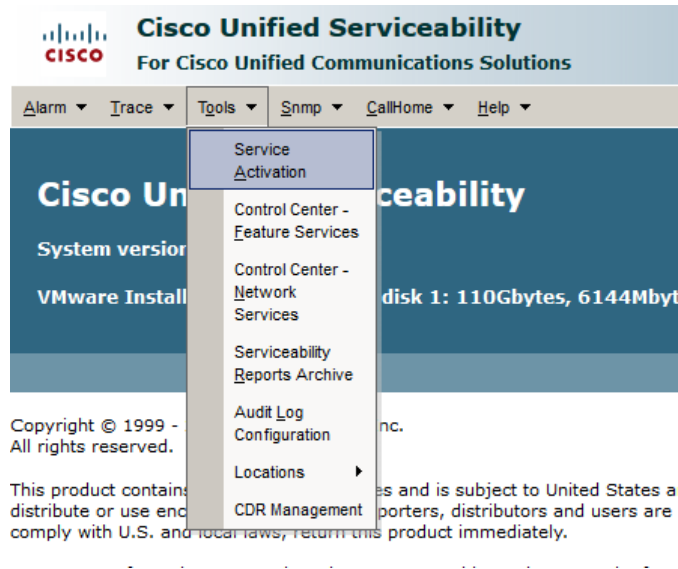
Este servicio es necesario para ejecutar búsquedas en directorios.



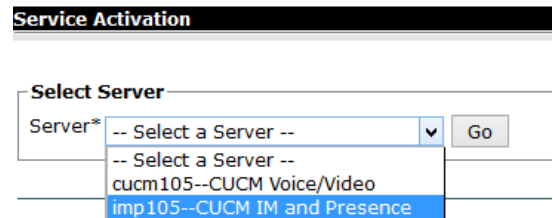
Este servicio es necesario para sincronizar con cualquier directorio como un LDAP.

**Nota: Ahora en la versión 10.x en adelante, el servidor de presencia IM&P es parte del cluster de CUCM, por lo tanto puedes acceder a los servicios de IM&P y CUCM desde la misma página de administración.**

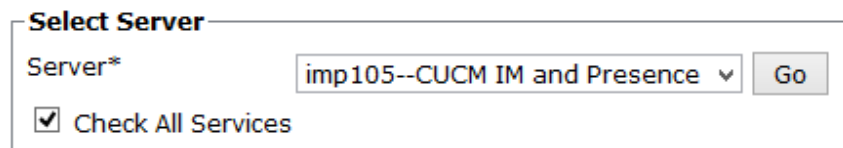
Seleccionamos **Tools> Service Activation** en el menú.



Seleccionamos nuestro servidor de presencia.



Seleccionamos la casilla **Check all Services** para que seleccione todos los servicios y activarlos. Hacemos click en **Save**.



## Agregar fotos a los usuarios de Active Directory

Podemos agregar la foto del usuario en Active Directory para que aparezcan las fotos de los contactos en el cliente de Jabber Windows.

Para clientes Jabber Windows usaremos el tipo de directorio EDI

EDI: Enhanced Directory Integration, es basado en Active Directory y otros directorios LDAP

Jabber busca las fotos en el atributo "jpegPhoto" o "thumbnailPhoto" para cada usuario.

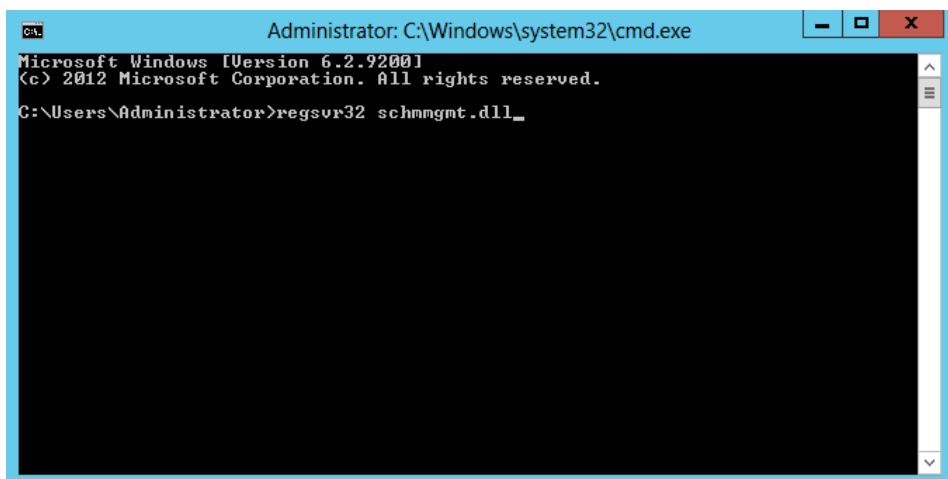
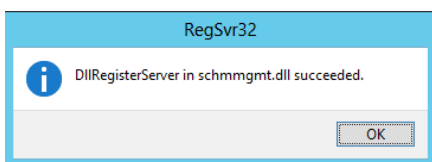
**Para usar estos tributos jpegPhoto ó thumbnailPhoto, se debe asegurar de que estos atributos se añaden al catálogo global en Active Directory.**

Para añadir los atributos de jpegPhoto y/o thumbnailPhoto al catálogo global hacemos lo siguiente:

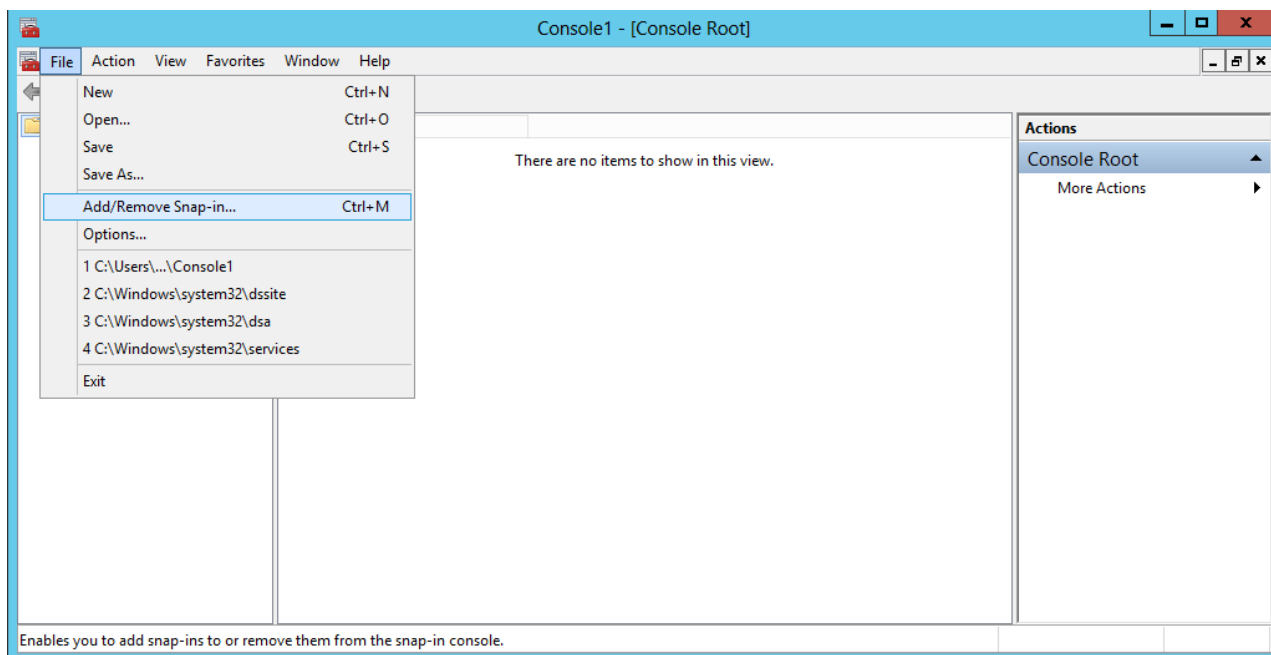
En nuestro Servidor de AD, abrimos una ventana de **CMD**, con permisos de administrador y tecleamos:

**regsvr32 schmmgmt.dll**

hacemos click en enter y nos aparece que fue exitoso.



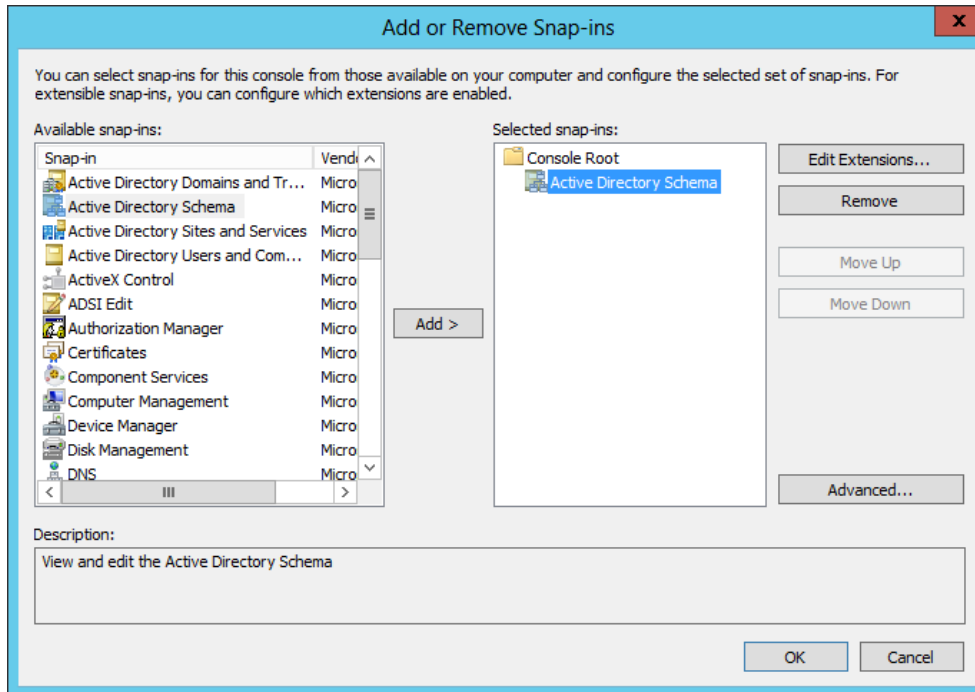
Ahora hacemos click en **Start** , **RUN**, y escribimos **MMC** y nos aparece esta ventana:



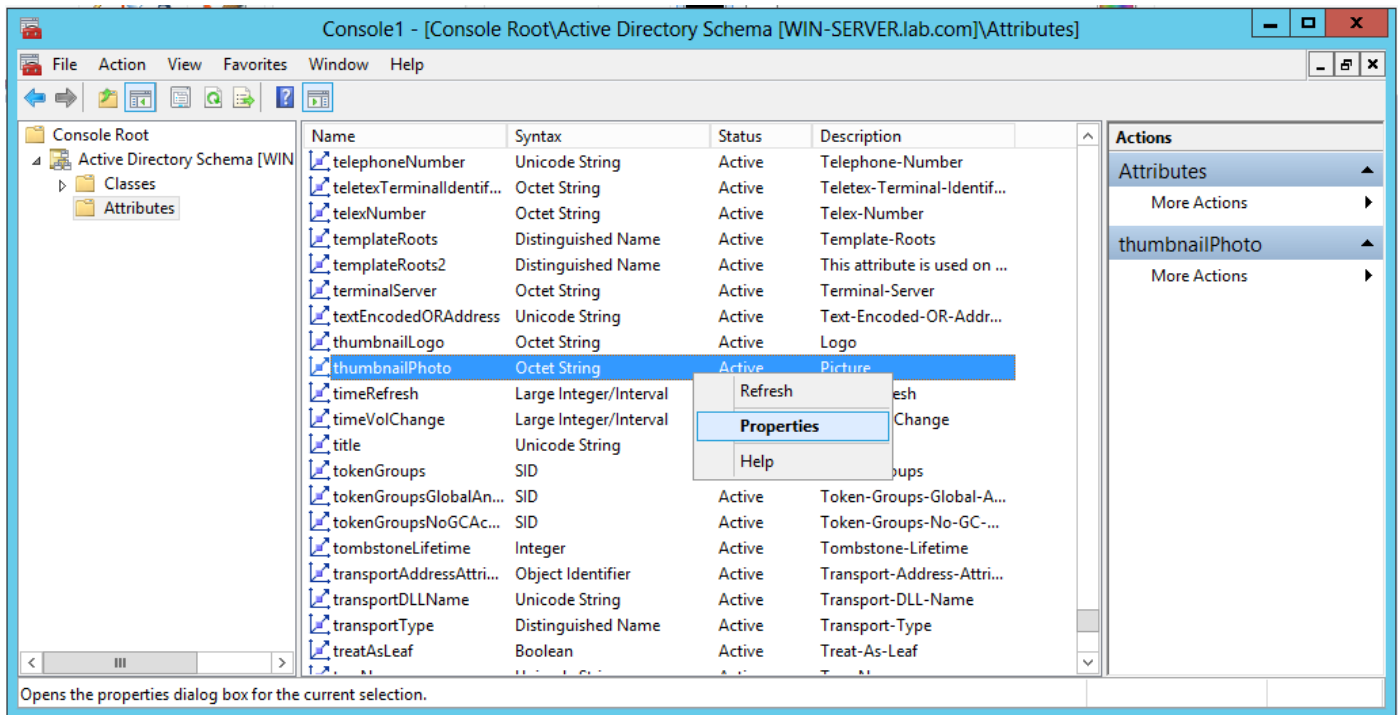
Vamos a **File**> **Add/Remove Snap-in...**



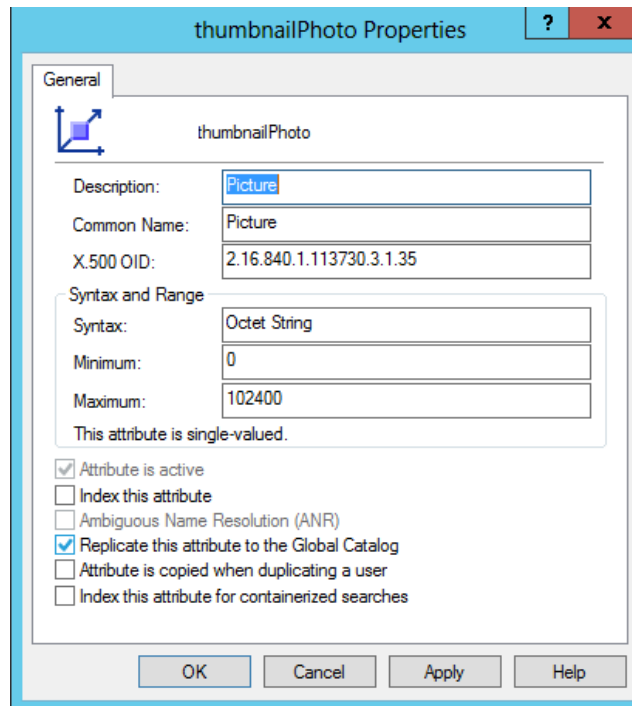
En esta ventana agregamos **Active Directory Schema** y hacemos clic en **OK**



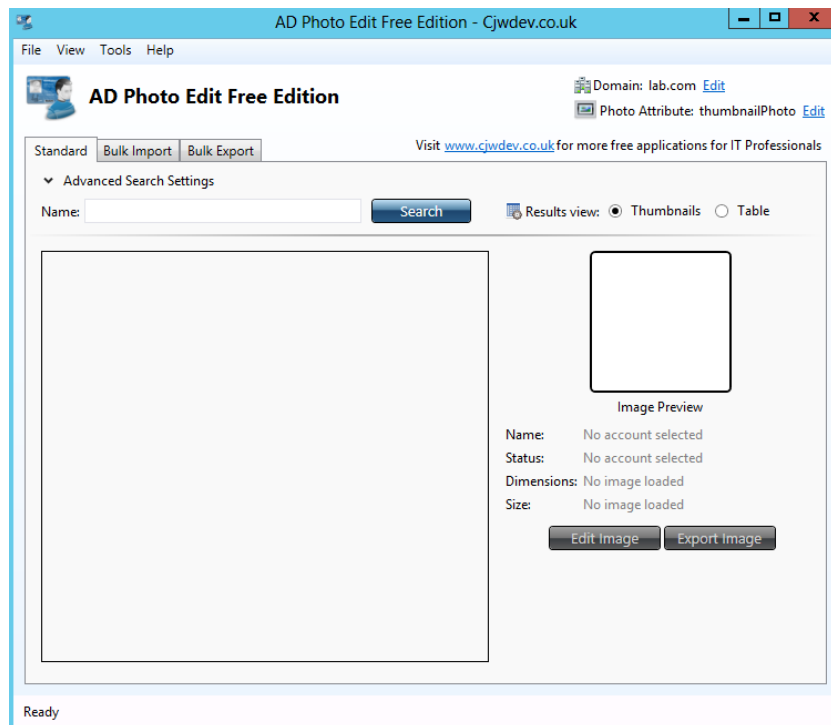
Nos regresa a la ventana anterior y seleccionamos a la derecha la carpeta **Attributes** , en la parte de en medio buscamos el atributo **"thumbnailPhoto"** y hacemos click derecho en **Properties**.



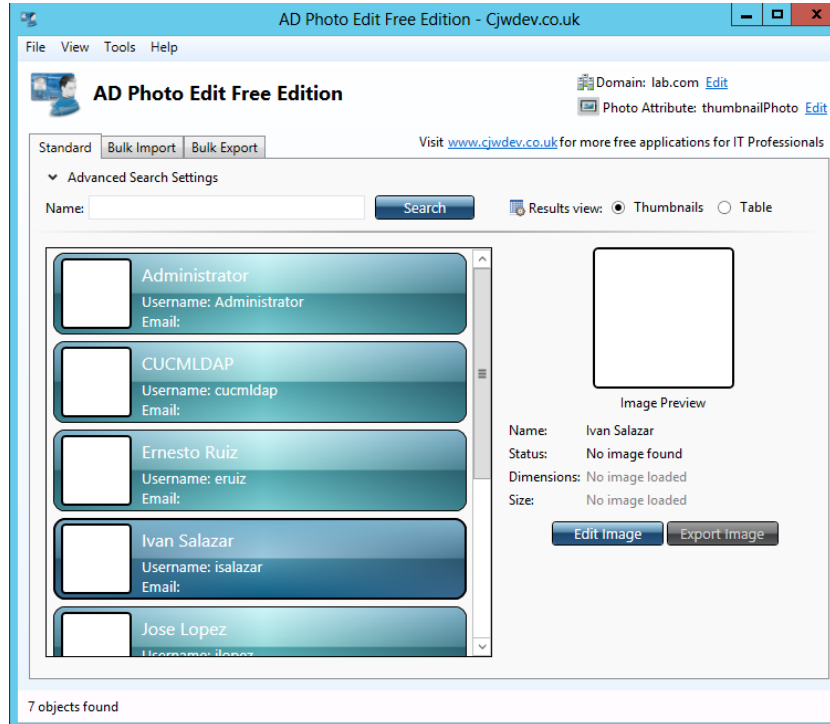
Ya nada más seleccionamos la casilla **“Replicate this attribute to the Global Catalog”**. Hacemos clic en **OK** y guardamos.



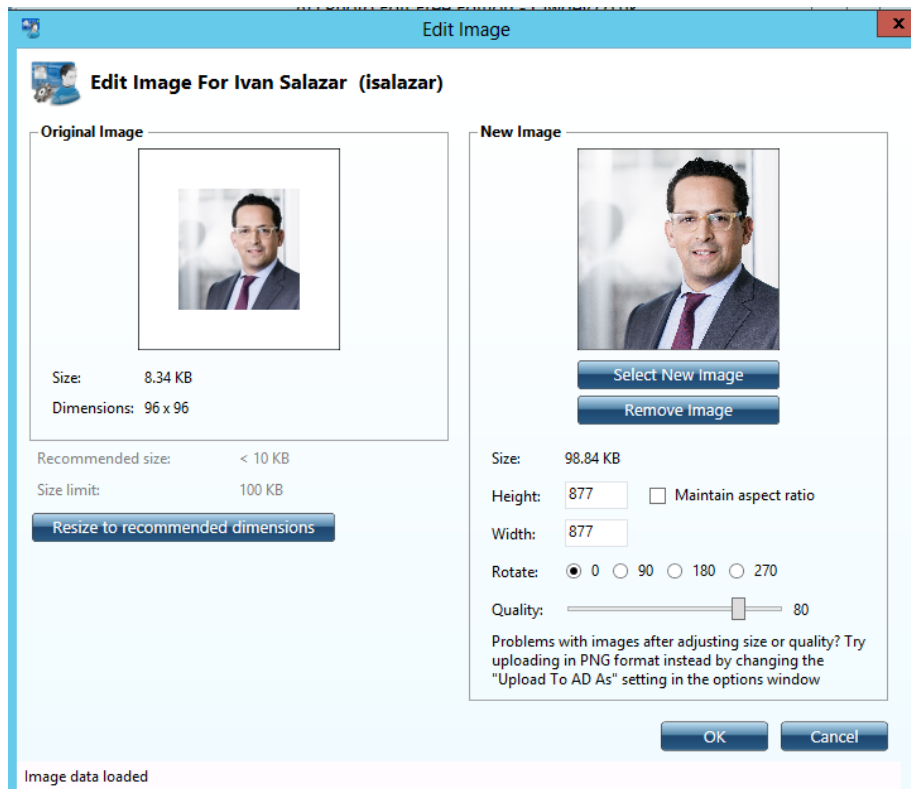
Podemos utilizar este software para agregar las fotos a los usuarios, lo instalamos en nuestro servidor AD, hacemos clic en **search** y nos busca los usuarios del dominio.



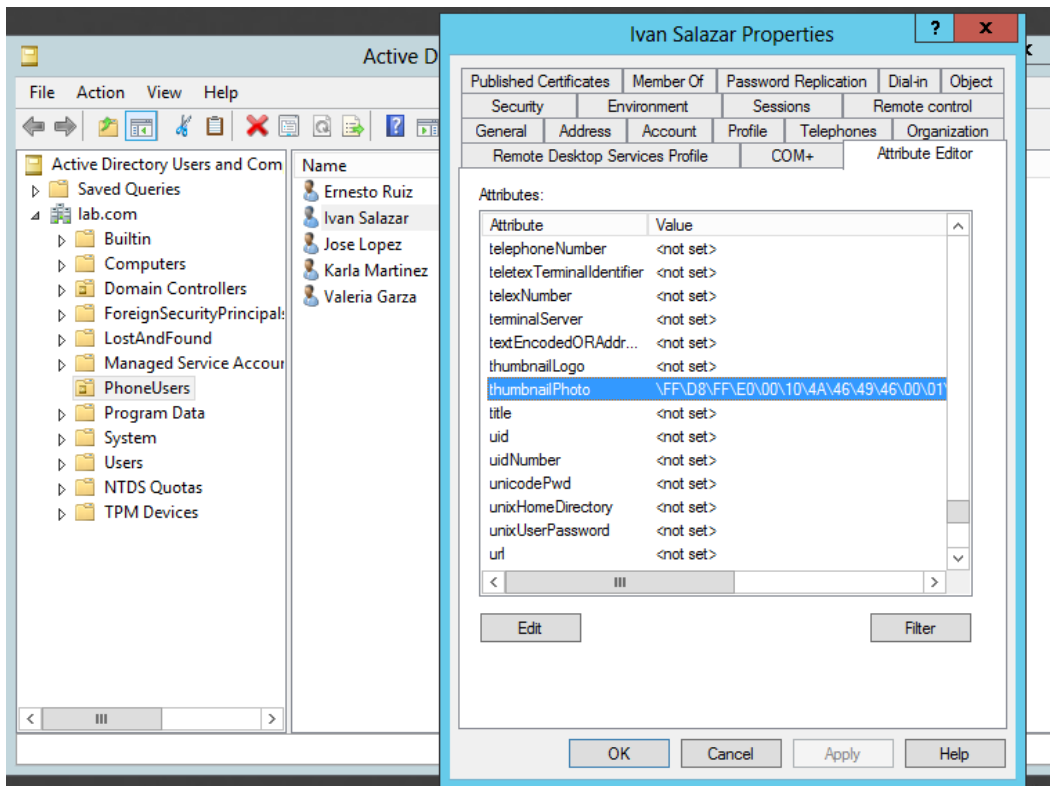
Seleccionamos el usuario para cargar la foto y hacemos clic en **Edit image**.



Seleccionamos la imagen y podemos indicar que ajuste al tamaño y dimensiones recomendados.



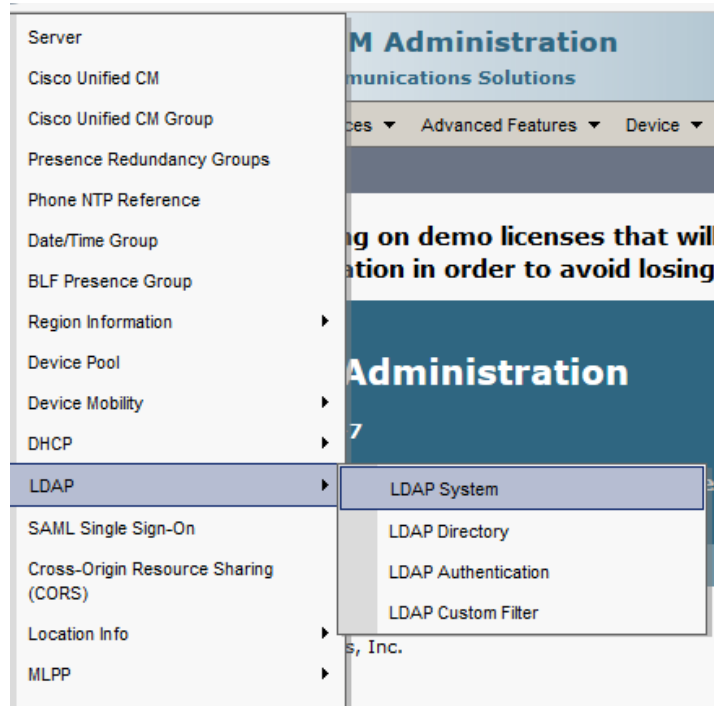
Para comprobar que la imagen se subió correctamente en las propiedades de usuarios, en la pestaña, **Attribute Editor**, en el atributo **thumbnailPhoto** hay un valor que guarda en hexadecimal, que es la foto que subimos.




Asi Jabber Windows busca los valores de las fotos dentro del AD.

## Sincronización con LDAP

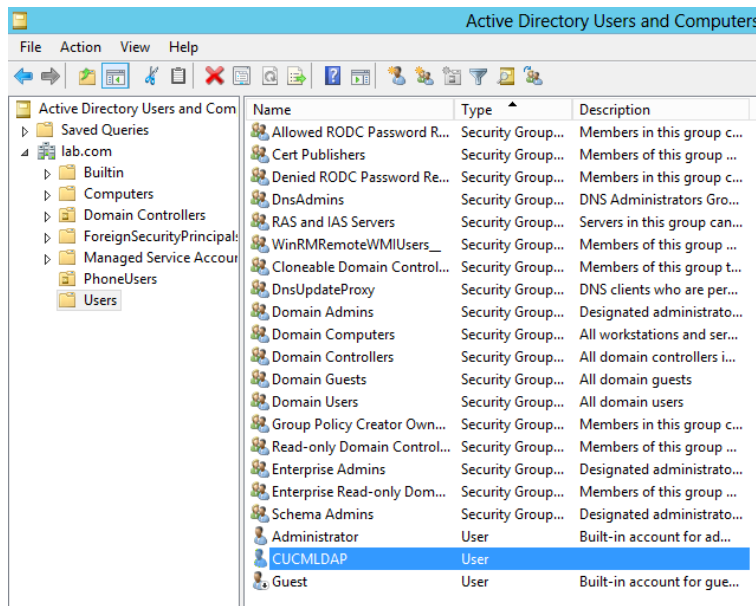
Para activar la sincronización con LDAP vamos **System > LDAP > LDAP System**.



Activamos la casilla y configuramos estas opciones.

<b>Status</b>	
	Status: Ready
<b>LDAP System Information</b>	
<input checked="" type="checkbox"/>	Enable Synchronizing from LDAP Server
LDAP Server Type	Microsoft Active Directory
LDAP Attribute for User ID	sAMAccountName

**Nota: Para importar los usuarios del directorio se necesita crear una cuenta con permisos de lectura que nos permita leer los objetos dentro de los directorios.**



Vamos a **System > LDAP > LDAP Directory**, y agregamos uno nuevo.

**LDAP Configuration Name**  
Solo ponemos un nombre

**LDAP Manager Distinguished Name**  
Ponemos el nombre de la cuenta de active directory

**LDAP password**  
El password de la cuenta

**LDAP User Search Base**  
Nuestra OU donde están los usuarios

**Phone Number**  
ipPhone

**Directory URI**  
mail

**LDAP Directory**

Save

LDAP Configuration Name\* CUCM-AD

LDAP Manager Distinguished Name\* CUCMLDAP@lab.com

LDAP Password\* .....

Confirm Password\* .....

LDAP User Search Base\* ou=PhoneUsers,dc=lab,dc=com

LDAP Custom Filter < None >

---

**LDAP Directory Synchronization Schedule**

Perform Sync Just Once

Perform a Re-sync Every\* 7 DAY

Next Re-sync Time (YYYY-MM-DD hh:mm)\* 2016-02-14 00:00

---

**Standard User Fields To Be Synchronized**

Cisco Unified Communications Manager User Fields	LDAP Attribute
User ID	sAMAccountName
Middle Name	middleName
Manager ID	manager
Phone Number	ipPhone
Title	title
Mobile Number	mobile
Directory URI	mail

**Host Name or IP Address for Server**  
La ip de nuestro Active Directory

**LDAP Server Information**

Host Name or IP Address for Server\* 10.10.10.10

LDAP Port\* 389

Use SSL

Add Another Redundant LDAP Server

Para poder loguearnos en Jabber necesitamos activar la autenticación de LDAP.

Nos vamos a **System >LDAP >LDAP Authentication**

Activamos la casilla

**Use LDAP Authentication for End Users**

**LDAP Manager Distinguished Name**

Ponemos el nombre de la cuenta de active directory

**LDAP password**

El password de la cuenta

**LDAP User Search Base**

Nuestra OU donde están los usuarios

**Host Name or IP Address for Server**

La ip de nuestro Active Directory

**LDAP Authentication for End Users**

Use LDAP Authentication for End Users

LDAP Manager Distinguished Name\* CUCMLDAP@lab.com

LDAP Password\* .....

Confirm Password\* .....

LDAP User Search Base\* ou=PhoneUsers,dc=lab,dc=com

**LDAP Server Information**

Host Name or IP Address for Server\* 10.10.10.10

LDAP Port\* 389

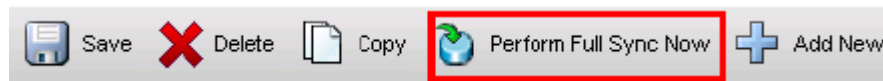
Use SSL

Add Another Redundant LDAP Server

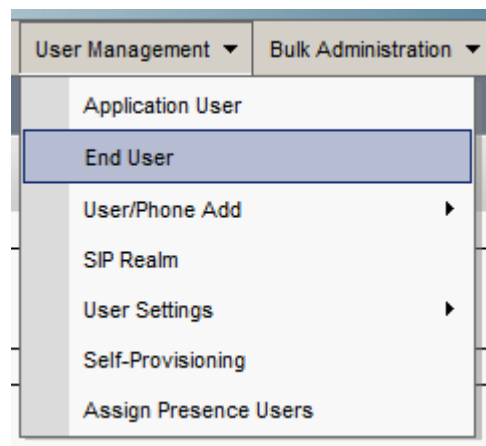
Para sincronizar los usuarios de AD hacia el CUCM , hacemos lo siguiente:

En **System > LDAP > LDAP Directory**

Activamos la casilla **Perform Sync Just Once** y después hacemos click en **Perform Full Sync Now**



Para comprobar la sincronización de los usuarios nos vamos a **User Management > End User**

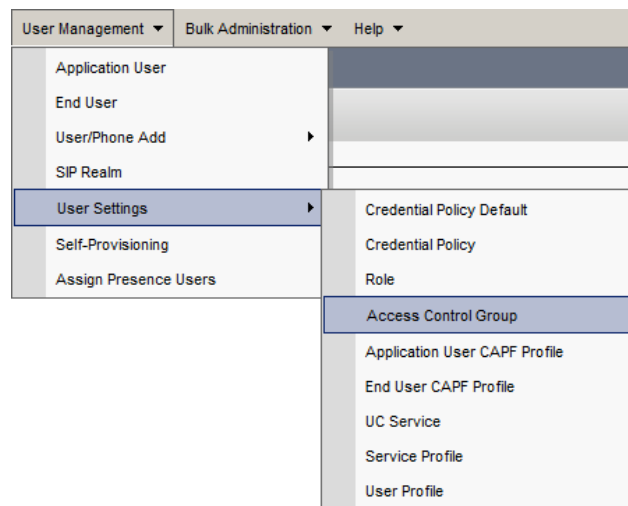


Ya vemos que nos aparecen los usuarios.

User (1 - 5 of 5)			
Find User where <input type="text" value="First name"/> <input type="text" value="begins with"/> <input type="button" value="Find"/> <input type="button" value="Clear Filter"/>			
<input type="checkbox"/>	User ID ^	First Name	
<input type="checkbox"/>	<a href="#">eruiz</a>	Ernesto	Ruiz
<input type="checkbox"/>	<a href="#">isalazar</a>	Ivan	Salazar
<input type="checkbox"/>	<a href="#">ilopez</a>	Jose	Lopez
<input type="checkbox"/>	<a href="#">kmartinez</a>	Karla	Martinez
<input type="checkbox"/>	<a href="#">vqarza</a>	Valeria	Garza

Todos los usuarios que creamos tenemos que ponerlos en el grupo **Standard CCM End Users** para que se loguen en su **End user web page**.

Para esto nos dirigimos a **User Management > User Settings > Access Control Group**

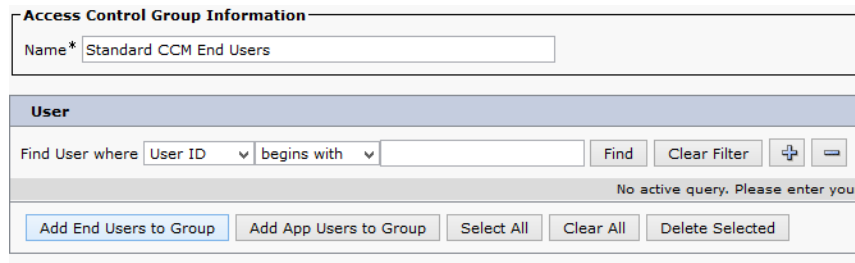




Hacemos click en **Find** y seleccionamos **Standard CCM End Users**



Hacemos click en **Add End Users to Group**

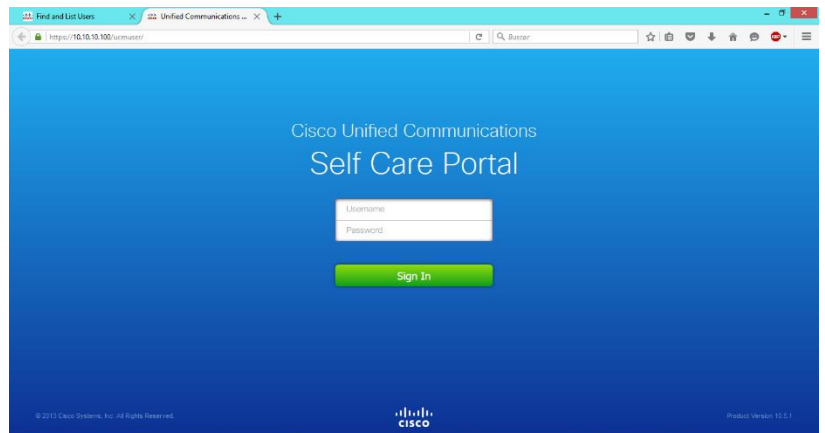


Le damos click en **Find** y **Select All** para seleccionar todos los usuarios, después en **Add Selected** para agregar todos los usuarios al grupo.

Para comprobar abrimos una ventana del navegador y escribimos la siguiente dirección:

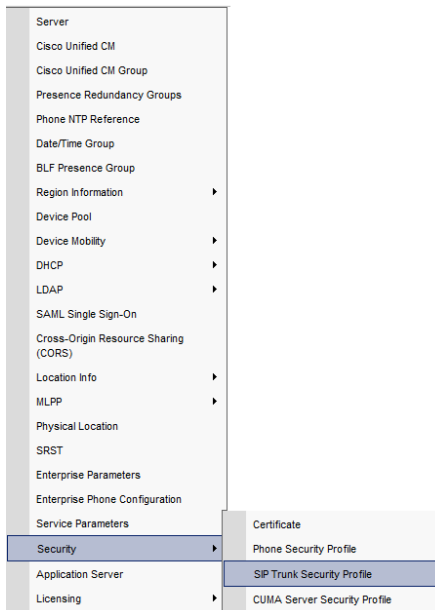
**https:// (ip call manager) /ucmuser**

Probamos con las credenciales de un usuario y nos debe de dar acceso a la página del usuario.

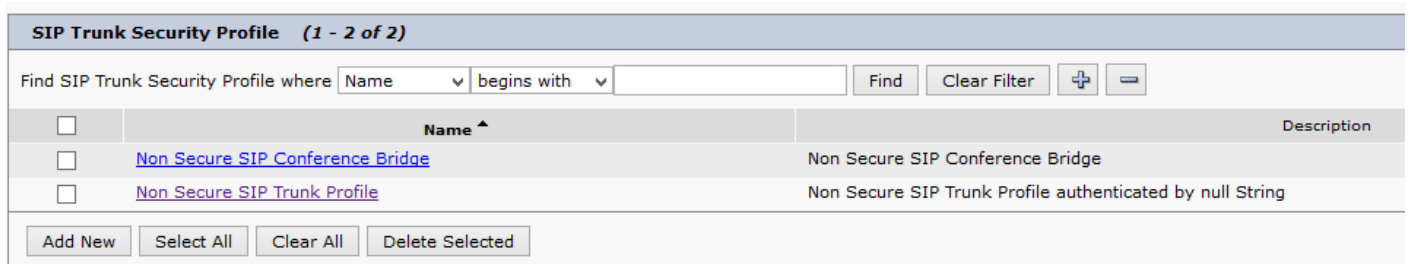


## Configuración SIP TRUNK SECURITY PROFILE

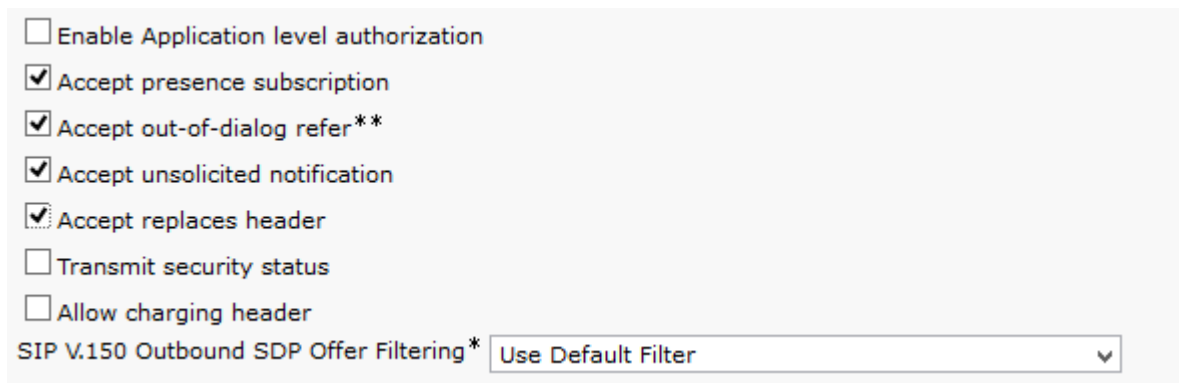
Para configurar el SIP Trunk Security Profile, nos vamos a **System > Security > SIP Trunk Security Profile**



Hacemos click en **Find** y seleccionamos **Non Secure SIP Trunk Profile**



Y habilitamos estas opciones; y guardamos.



# Configuración de SIP Trunk hacia IM&P Server

Vamos hacia **Device > Trunk**

Device ▾

- CTI Route Point
- Gatekeeper
- Gateway
- Phone
- Trunk**
- Remote Destination
- Device Settings ▶

**Trunk Information**

Trunk Type*	SIP Trunk ▾
Device Protocol*	SIP ▾
Trunk Service Type*	None(Default) ▾

Y los configuramos con estos parámetros:

- Device Name:** ponemos un nombre.
- Description:** descripción.
- Device pool:** nuestro device pool.

**Device Information**

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	Presence-SIP-Trunk
Description	SIP Trunk to Presence
Device Pool*	Monterrey ▾
Common Device Configuration	< None > ▾
Call Classification*	Use System Default ▾
Media Resource Group List	< None > ▾
Location*	Hub_None ▾
AAR Group	< None > ▾
Tunneled Protocol*	None ▾
QSIG Variant*	No Changes ▾
ASN.1 ROSE OID Encoding*	No Changes ▾
Packet Capture Mode*	None ▾
Packet Capture Duration	0

**Destination Address:**  
Hostname de nuestro servidor IM&P.

**SIP Trunk Security Profile:**  
Non Secure SIP Trunk Profile.

**SIP Profile:**  
Standard SIP Profile.

**Destination**

Destination Address is an SRV

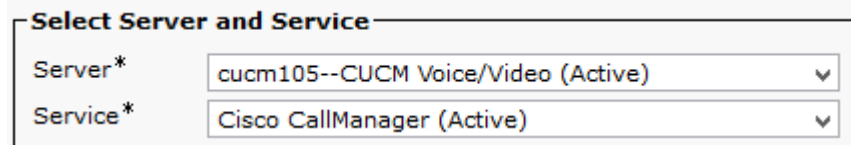
1*	Destination Address	Destination Address IPv6	Destination Port
	imp105		5060

MTP Preferred Originating Codec*	711ulaw ▾
BLF Presence Group*	Standard Presence group ▾
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile ▾
Rerouting Calling Search Space	< None > ▾
Out-Of-Dialog Refer Calling Search Space	< None > ▾
SUBSCRIBE Calling Search Space	< None > ▾
SIP Profile*	Standard SIP Profile ▾ <a href="#">View Details</a>
DTMF Signaling Method*	No Preference ▾

## Seleccionar IM&P Publish Trunk

Le indicamos al CUCM que publish trunk debe de usar.

Nos vamos a **System > Service Parameters** y seleccionamos el servidor CUCM y el servicio **CallManager**

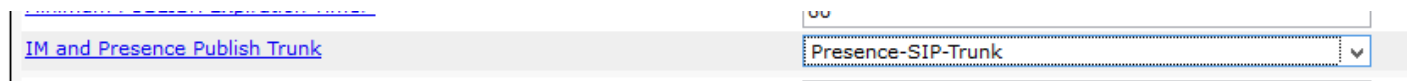


**Select Server and Service**

Server\*

Service\*

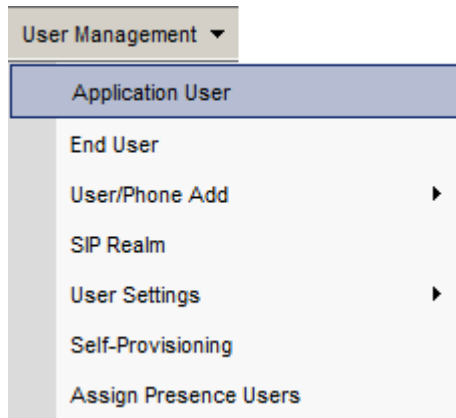
Bajamos hasta **Clusterwide Parameters ( Device –SIP )** y seleccionamos nuestro SIP Trunk.



**IM and Presence Publish Trunk**

## AXL Application User

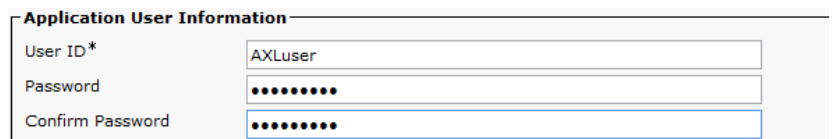
Vamos a crear un usuario para comunicar al CUCM con el IM&P Server, para eso vamos a **User Management > Application User**.



**User Management**

- Application User
- End User
- User/Phone Add
- SIP Realm
- User Settings
- Self-Provisioning
- Assign Presence Users

Le ponemos un nombre y una contraseña.



**Application User Information**

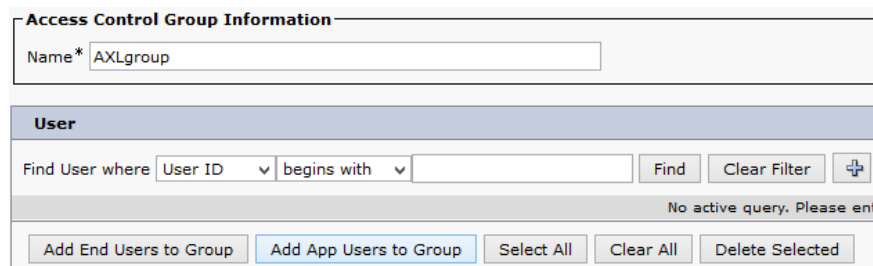
User ID\*

Password

Confirm Password

Ahora creamos un nuevo **User Group** y le agregamos el **Application User** que acabamos de crear.

Vamos a **User Management > UserSettings > Access Control Group**.



**Access Control Group Information**

Name\*

**User**

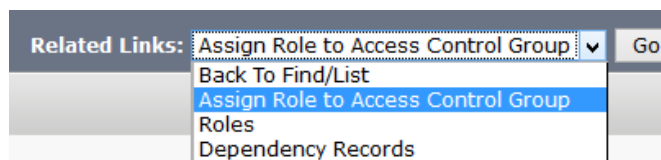
Find User where  begins with

No active query. Please enter a query.

Hacemos click en **Add App Users to Group** y seleccionamos el que acabamos de crear y guardamos.

<input type="checkbox"/>	User ID ^
<input checked="" type="checkbox"/>	<a href="#">AXLuser</a>
<input type="checkbox"/>	<a href="#">Administrator</a>
<input type="checkbox"/>	<a href="#">CCMORTSecureSysUser</a>
<input type="checkbox"/>	<a href="#">CCMORTSysUser</a>
<input type="checkbox"/>	<a href="#">CCMSysUser</a>
<input type="checkbox"/>	<a href="#">CUCService</a>
<input type="checkbox"/>	<a href="#">IPMAMSecureSysUser</a>

Después en esa misma ventana seleccionamos **Assign Role to Access Control Group**.



Y hacemos click en **Assign Role to Group**.

**Role Assignment**

Role

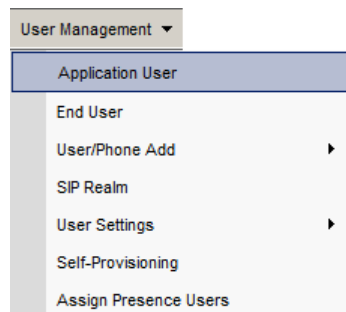
Y seleccionamos **Standard AXL API Access** y guardamos.

<input type="checkbox"/>		configuration
<input checked="" type="checkbox"/>	<a href="#">Standard AXL API Access</a>	Cisco Call Manager AXL Database Access the AXL APIs

## CTI Application User

Vamos a crear un grupo que se llamara CTI group , esto es para que Jabber reconozca si tienes asociado un teléfono y puedas controlarlo desde el cliente de Jabber.

Para esto vamos a **User Management > Application User**.



Le ponemos un nombre y una contraseña.

**Application User Information**

User ID\*

Password

Confirm Password

Digest Credentials

Vamos a **User Management > UserSettings > Access Control Group** para crear un grupo , agregamos uno nuevo y escribimos un nombre.

**Access Control Group Information**

Name\* CTIgroup

**User**

Find User where User ID begins with Find Clear Filter

No active query. Please enter your s

Add End Users to Group Add App Users to Group Select All Clear All Delete Selected

Hacemos click en **Add App Users to Group** y seleccionamos el que acabamos de crear **CTIuser** guardamos.

**Application User (1 - 13 of 13)** Rows per Page

Find Application User where User ID begins with Find Clear Filter

<input type="checkbox"/>	User ID ^	Co
<input type="checkbox"/>	<a href="#">AXLuser</a>	
<input type="checkbox"/>	<a href="#">Administrator</a>	
<input type="checkbox"/>	<a href="#">CCMORTSecureSysUser</a>	
<input type="checkbox"/>	<a href="#">CCMORTSysUser</a>	
<input type="checkbox"/>	<a href="#">CCMSysUser</a>	
<input checked="" type="checkbox"/>	<a href="#">CTIuser</a>	
<input type="checkbox"/>	<a href="#">CUCService</a>	
<input type="checkbox"/>	<a href="#">IPMASecureSysUser</a>	
<input type="checkbox"/>	<a href="#">IPMA...</a>	

Después en esa misma ventana seleccionamos **Assign Role to Access Control Group**.

**Related Links:** Assign Role to Access Control Group Go

- Back To Find/List
- Assign Role to Access Control Group
- Roles
- Dependency Records

Y hacemos click en **Assign Role to Group**.

**Role Assignment**

Role

Assign Role to Group

Delete Role Assignment

Y seleccionamos los CTI que aparecen en la imagen

Role Name	Role Type	Description	Actions
<input type="checkbox"/> <a href="#">Standard System Service Management</a>	Cisco Call Manager Serviceability	Standard System Service Management	
<input checked="" type="checkbox"/> <a href="#">Standard CTI Allow Call Monitoring</a>	Cisco Computer Telephone Interface (CTI)	Allow monitoring of calls	
<input checked="" type="checkbox"/> <a href="#">Standard CTI Allow Call Park Monitoring</a>	Cisco Computer Telephone Interface (CTI)	Allow monitoring of call park DN's	
<input checked="" type="checkbox"/> <a href="#">Standard CTI Allow Call Recording</a>	Cisco Computer Telephone Interface (CTI)	Allow recording of calls	
<input checked="" type="checkbox"/> <a href="#">Standard CTI Allow Calling Number Modification</a>	Cisco Computer Telephone Interface (CTI)	Allow calling number modification	
<input checked="" type="checkbox"/> <a href="#">Standard CTI Allow Control of All Devices</a>	Cisco Computer Telephone Interface (CTI)	Allow control of all CTI controllable devices	
<input checked="" type="checkbox"/> <a href="#">Standard CTI Allow Control of Phones supporting Connected Xfer and conf</a>	Cisco Computer Telephone Interface (CTI)	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	
<input checked="" type="checkbox"/> <a href="#">Standard CTI Allow Control of Phones supporting Rollover Mode</a>	Cisco Computer Telephone Interface (CTI)	Standard CTI Allow Control of Phones supporting Rollover Mode	
<input type="checkbox"/> <a href="#">Standard CTI Allow Reception of SRTP Key Material</a>	Cisco Computer Telephone Interface (CTI)	Allows access to SRTP key material	
<input checked="" type="checkbox"/> <a href="#">Standard CTI Enabled</a>	Cisco Computer Telephone Interface (CTI)	Enable CTI application control	
<input type="checkbox"/> <a href="#">Standard CTI Secure Connection</a>	Cisco Computer Telephone Interface (CTI)	Application connection to CTI/CM must be secure	
<input type="checkbox"/> <a href="#">Standard EM Authentication Proxy</a>	Cisco Extension	Manages EM Authentication	

## Creación de Dispositivos

Podemos configurar el cliente de Jabber en diferentes dispositivos, como PC, MAC, iPhone, Android, Tablets, iPads, cada uno requiere crear un dispositivo diferente.

Configuración cliente Jabber Windows:

Vamos a **Device > Phone**. Y agregamos uno nuevo (para Windows es **Client Services Framework**, CFS).

Select the type of phone you would like to create

Phone Type\*

En el nombre del dispositivo debe de ponerse de esta manera: CFS+ nombre

Llenamos los demás campos como si fuera un teléfono más, particiones, CSS, location, etc

Phone Type	
<b>Product Type:</b>	Cisco Unified Client Services Framework
<b>Device Protocol:</b>	SIP
Device Information	
<input checked="" type="checkbox"/> Device is trusted	
Device Name*	CSFIsalazar
Description	Jabber Ivan Salazar
Device Pool*	Monterrey <a href="#">View Details</a>
Common Device Configuration	< None > <a href="#">View Details</a>
Phone Button Template*	Standard Client Services Framework
Common Phone Profile*	Standard Common Phone Profile <a href="#">View Details</a>
Calling Search Space	EXTENCIONES
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
AAR Group	< None >

En **Owner** seleccionamos **User** y **Owner User ID**, el ID del usuario al que se le configura el softphone.

En **Primary Phone** la mac address del teléfono físico que tiene asociado ese usuario.

AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
AAR Group	< None >
User Locale	< None >
Network Locale	< None >
Built In Bridge*	Default
Device Mobility Mode*	Default <a href="#">View Current Device M</a>
Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)
Owner User ID*	isalazar
Mobility User ID	< None >
Primary Phone	SEP001122334455
Use Trusted Relay Point*	Default
Always Use Prime Line*	Default
Always Use Prime Line for Voice Message*	Default
Geolocation	< None >



Bajamos hasta **Protocol Specific Information**

En **Device Security Profile** seleccionamos **Cisco Unified Client Services Framework Standard**

En **SIP Profile** seleccionamos **Standard SIP Profile**

En **Digest User** el ID del usuario.

**Protocol Specific Information**

Packet Capture Mode\*

Packet Capture Duration

BLF Presence Group\*

SIP Dial Rules

MTP Preferred Originating Codec\*

Device Security Profile\*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile\*  [View Details](#)

Digest User

Media Termination Point Required

Unattended Port

Require DTMF Reception

Hacemos click en Guardar y aplicar, para guardar los cambios.

Le asignamos una extensión al cliente de Jabber

**Line [1] – Add a new DN**

**Directory Number Information**

Directory Number\*   Urgent Priority

Route Partition

Description

Alerting Name

ASCII Alerting Name

External Call Control Profile

Allow Control of Device from CTI

Associated Devices

Dissociate Devices

Y asociamos la extensión con el end user.

**Multiple Call/Call Waiting Settings on Device CSFIsalazar**

Note: The range to select the Max Number of calls is: 1-6

Maximum Number of Calls\*

Busy Trigger\*  (Less than or equal to Max. C

**Forwarded Call Information Display on Device CSFIsalazar**

Caller Name

Caller Number

Redirected Number

Dialed Number

**Users Associated with Line**

	Full Name	User ID
<input type="checkbox"/>	Salazar, Ivan	isalazar

Ahora nos vamos a **User Management > End User**, aquí vamos a asociar los dispositivos con el usuario final, Seleccionamos **Device Association**

Y seleccionamos los dispositivos que queremos asociar al usuario final, click en **Save Selected /Changes**

**User Device Association (1 - 3 of 3)**

Find User Device Association where Name begins with  Find Clear Filter

Show the devices already associated with user

<input type="checkbox"/>		Device Name	Directory Number	
<input checked="" type="checkbox"/>		SEP001122334455	1210	Ivan Salazar
<input checked="" type="checkbox"/>		CSFIsalazar	1210	Jabber Ivan Salazar
<input type="checkbox"/>		SEP112233445566	2210	Jose Lopez

Select All Clear All Select All In Search Clear All In Search **Save Selected/Changes** Remove All Associated

Hasta la parte de abajo nos vamos a la sección **Permissions Information** y seleccionamos **Add to Access Control Group**

Y seleccionamos los grupos que creamos, **AXLgroup** y **CTIgroup**

**Access Control Group (1 - 29 of 29)**

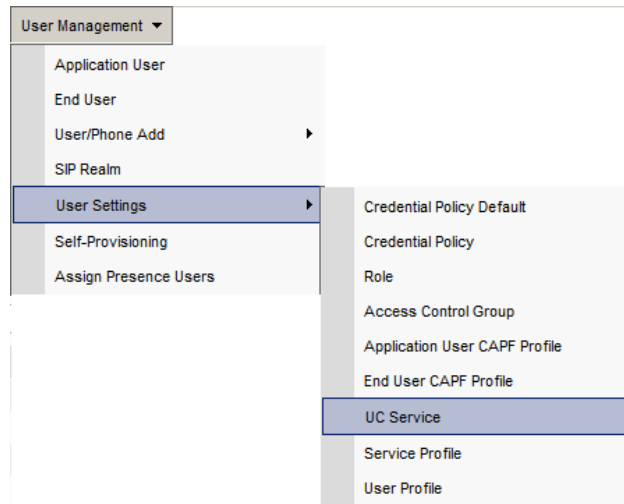
Find Access Control Group where Name begins with

<input type="checkbox"/>	Name ^
<input checked="" type="checkbox"/>	AXLgroup
<input type="checkbox"/>	Admin-3rd Party API
<input type="checkbox"/>	Application Client Users
<input checked="" type="checkbox"/>	CTIgroup
<input type="checkbox"/>	Standard Audit Users
<input type="checkbox"/>	Standard CAR Admin Users
<input type="checkbox"/>	Standard CCM Admin Users
<input type="checkbox"/>	Standard CCM Gateway Administration
<input type="checkbox"/>	Standard CCM Phone Administration
<input type="checkbox"/>	Standard CCM Read Only

## Crear UC Services

El cliente de Jabber cuando inicia, busca la configuración, configuramos servicios como voicemail, CTI, Conference y los asociamos a un perfil que vamos a crear.

Vamos a **User management > User Settings > UC Service** y agregamos uno nuevo.



Seleccionamos CTI, y lo llenamos con la siguiente información:

**Host Name /IP Address** es la IP o host name de nuestro Call Manager.

UC Service Information	
<b>UC Service Type:</b>	CTI
<b>Product Type:</b>	CTI
Name*	<input type="text" value="CTI"/>
Description	<input type="text" value="CTI service"/>
Host Name/IP Address*	<input type="text" value="cucm105"/>
Port	<input type="text" value="2748"/>
<b>Protocol:</b>	TCP

Seleccionamos **IM and Presence**, y lo llenamos con la siguiente información:

**Host Name /IP Address** es la IP o host name de nuestro IM&P Server.

UC Service Information	
<b>UC Service Type:</b>	<b>IM and Presence</b>
Product Type*	Unified CM (IM and Presence) ▼
Name*	IMP
Description	IMP Service
Host Name/IP Address*	imp105

Seleccionamos **Directory** y lo llenamos con la siguiente información:

**Host Name /IP Address** es la IP o host name de nuestro Active Directory.

UC Service Information	
<b>UC Service Type:</b>	<b>Directory</b>
Product Type*	Directory ▼
Name*	Directory
Description	Directory Service
Host Name/IP Address*	win-server
Port	389
Protocol	TCP ▼

Esos son los servicios que configuraremos en este laboratorio.

Ahora vamos a crear un perfil para esos servicios, nos vamos a **User Management > User Settings > Service Profile**.

The screenshot shows a hierarchical menu structure. At the top is 'User Management' with a dropdown arrow. Below it are several options: 'Application User', 'End User', 'User/Phone Add' (with a right-pointing arrow), 'SIP Realm', 'User Settings' (with a right-pointing arrow and highlighted in blue), 'Self-Provisioning', and 'Assign Presence Users'. From the 'User Settings' option, a secondary menu is open, listing: 'Credential Policy Default', 'Credential Policy', 'Role', 'Access Control Group', 'Application User CAPF Profile', 'End User CAPF Profile', 'UC Service', 'Service Profile' (highlighted in blue), and 'User Profile'.

Creamos un perfil nuevo y le ponemos un nombre y una descripción.

Service Profile Information	
Name*	<input type="text" value="Jabber_lab"/>
Description	<input type="text" value="Jabber profile"/>
<input type="checkbox"/> Make this the default service profile for the system	

En la parte de **Directory Profile**, lo llenamos con la siguiente información,

**Username.-** Es el usuario que usamos para sincronizar con el Active Directory y el password

**Search Base 1.-** Es la unidad organizativa donde buscara los usuarios, es la misma que usamos en la integración con LDAP

Directory Profile	
Primary	<input type="text" value="Directory"/>
Secondary	<input type="text" value="&lt;None&gt;"/>
Tertiary	<input type="text" value="&lt;None&gt;"/>
<input type="checkbox"/> Use UDS for Contact Resolution	
<input type="checkbox"/> Use Logged On User Credential	
<a href="#">Username</a>	<input type="text" value="CUCMLDAP@lab.com"/>
<a href="#">Password</a>	<input type="password" value="••••••••"/>
<a href="#">Search Base 1</a>	<input type="text" value="ou=PhoneUsers, dc=lab, dc=com"/>
<a href="#">Search Base 2</a>	<input type="text"/>
<a href="#">Search Base 3</a>	<input type="text"/>
<input checked="" type="checkbox"/> Recursive Search on All Search Bases	
<a href="#">Search Timeout (seconds)*</a>	<input type="text" value="5"/>
<a href="#">Base Filter (Only used for Advance Directory)</a>	<input type="text"/>
<a href="#">Predictive Search Filter (Only used for Advance Directory)</a>	<input type="text"/>

Seleccionamos los servicios creados en el paso anterior...

IM and Presence Profile	
Primary	<input type="text" value="IMP"/>
Secondary	<input type="text" value="&lt;None&gt;"/>
Tertiary	<input type="text" value="&lt;None&gt;"/>

CTI Profile	
Primary	<input type="text" value="CTI"/>
Secondary	<input type="text" value="&lt;None&gt;"/>
Tertiary	<input type="text" value="&lt;None&gt;"/>

Ahora al usuario, en **User Management > End User** le asignamos el perfil de que acabamos de crear.

**Service Settings**

Home Cluster

Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

[Presence Viewer for User](#)

UC Service Profile:  [View Details](#)

## Configurar IM&P Server

Entramos al servidor

End User Configuration | IM and Presence Service C...

https://10.10.10.101/cupadmin/showHome.do

**Cisco Unified CM IM and Presence Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM IM and Presence Administration | Go

System | Presence | Messaging | Application | Bulk Administration | Diagnostics | Help

**Cisco Unified CM IM and Presence Administration**  
System version: 10.5.1.10000-9  
VMware Installation: -1 vCPU, disk 1: 80Gbytes, 4096Mbytes RAM

Copyright © 1999 - 2014 Cisco Systems, Inc.  
All rights reserved.

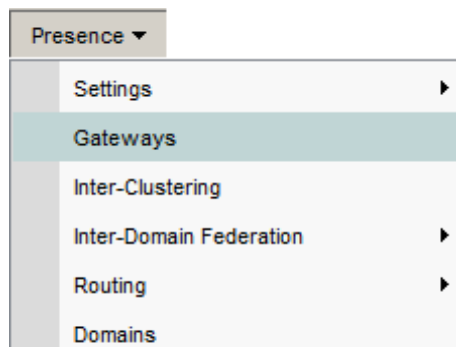
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

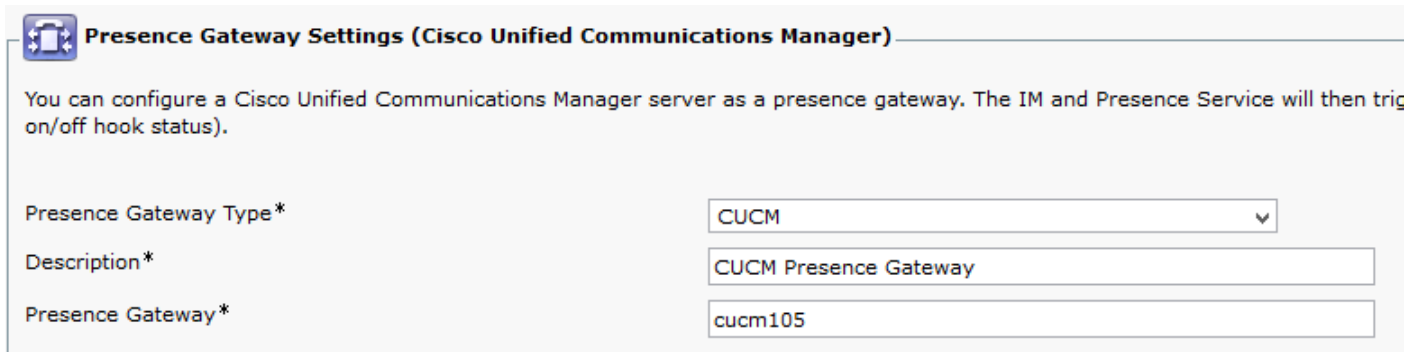
For information about Cisco Unified CM IM and Presence please visit our [IM and Presence Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Ahora nos vamos a **Presence > Gateways** y crear uno nuevo.



En **Presence Gateway Type** seleccionamos “**CUCM**” escribimos una descripción y en **Presence Gateway** escribimos la IP o hostname de nuestro Call Manager.



**Presence Gateway Settings (Cisco Unified Communications Manager)**

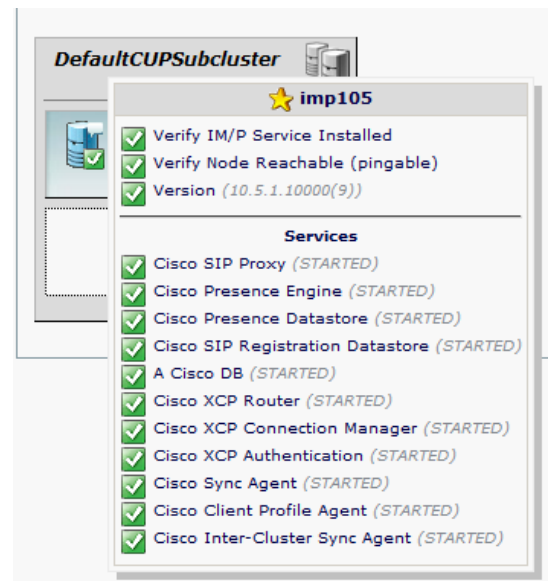
You can configure a Cisco Unified Communications Manager server as a presence gateway. The IM and Presence Service will then trigger on/off hook status).

Presence Gateway Type\*

Description\*

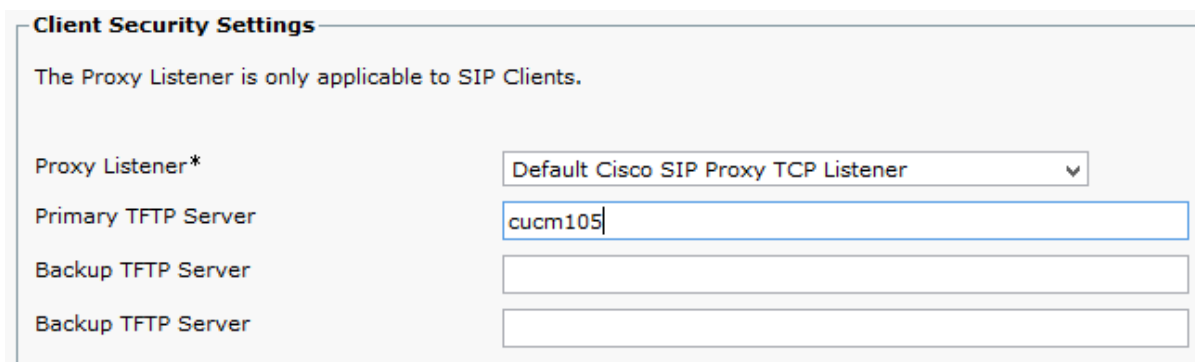
Presence Gateway\*

Para confirmar que todos los servicios están iniciados, vamos a **System > Presence Topology** y movemos el mouse sobre icono como de un servidor y nos mostrara esta imagen.



Nos dirigimos a **Application > Legacy Clients > Settings**

En **Primary TFTP Server**, seleccionamos la IP o Hostname de nuestro Call Manager.



**Client Security Settings**

The Proxy Listener is only applicable to SIP Clients.

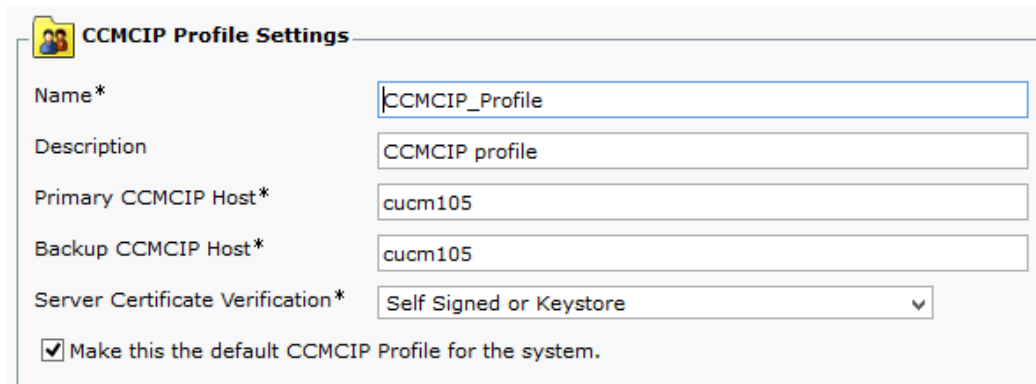
Proxy Listener\*

Primary TFTP Server

Backup TFTP Server

Backup TFTP Server

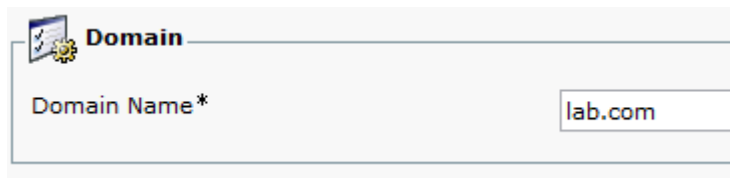
Ahora nos dirigimos a **Application > Legacy Clients > CCMCIP Profile** y agregamos uno nuevo  
En **Primary CCMCIP Host** seleccionamos la IP o Hostname de nuestro Call Manager.  
Seleccionamos **Make this the default CCMCIP Profile for the system**.



The screenshot shows the 'CCMCIP Profile Settings' window. It contains the following fields and options:

- Name\***: CCMCIP\_Profile
- Description**: CCMCIP profile
- Primary CCMCIP Host\***: cucm105
- Backup CCMCIP Host\***: cucm105
- Server Certificate Verification\***: Self Signed or Keystore (dropdown menu)
- Make this the default CCMCIP Profile for the system.**

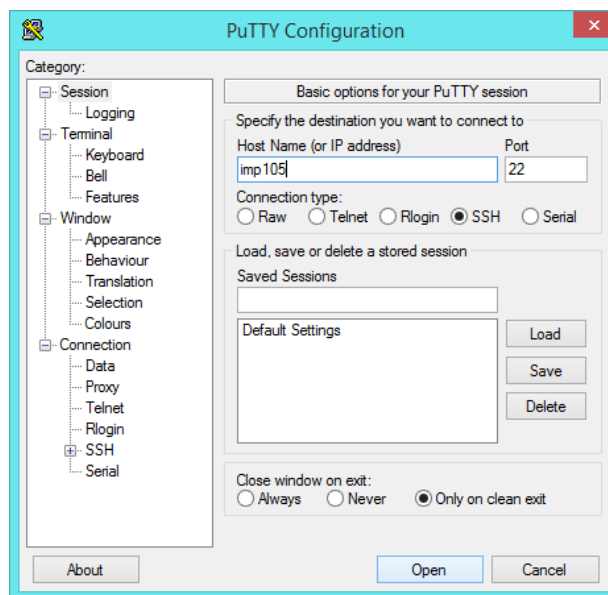
Vamos a agregar el dominio al servidor, nos vamos a **Presence > Domains**. En **Domain Name** escribimos nuestro dominio.



The screenshot shows the 'Domain' configuration window. It contains the following field:

- Domain Name\***: lab.com

Reiniciamos el servidor para que se apliquen los últimos cambios y sincronice los usuarios con el Call Manager  
Podemos usar el programa **Putty** y entramos por medio de **SSH**.



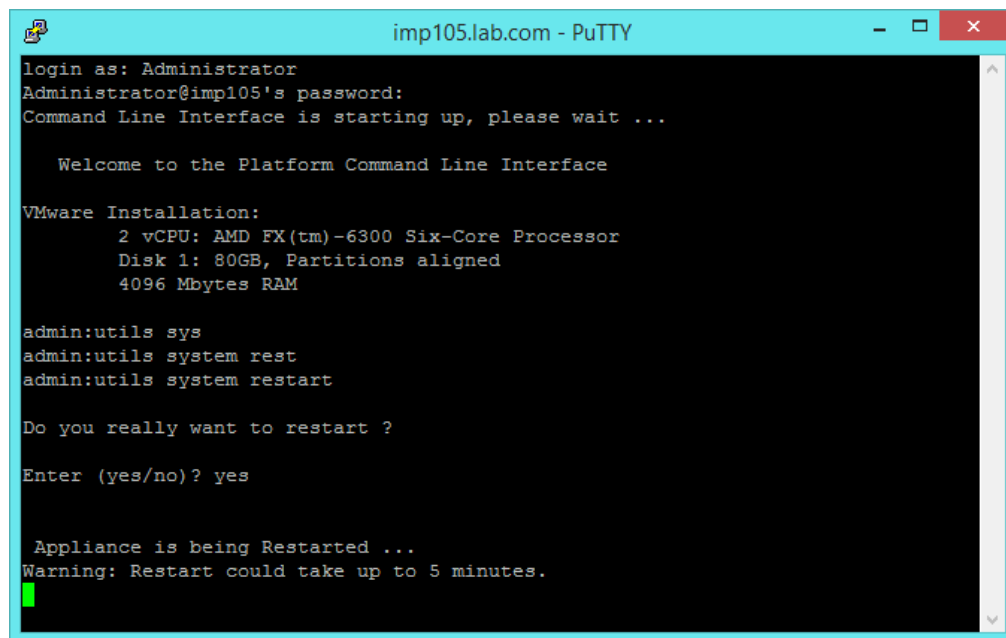
The screenshot shows the 'PuTTY Configuration' dialog box. The 'SSH' category is selected in the left-hand tree. The 'Basic options for your PuTTY session' section is expanded, showing the following settings:

- Host Name (or IP address)**: imp105
- Port**: 22
- Connection type**: SSH (selected with a radio button)
- Close window on exit**: Only on clean exit (selected with a radio button)

Buttons for 'Open' and 'Cancel' are visible at the bottom of the dialog.



Entramos con nuestro usuario y password y escribimos **“utils system restart”** y después confirmamos, y esperamos que se reinicie el servidor.



```
imp105.lab.com - PuTTY
login as: Administrator
Administrator@imp105's password:
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
 2 vCPU: AMD FX(tm)-6300 Six-Core Processor
 Disk 1: 80GB, Partitions aligned
 4096 Mbytes RAM

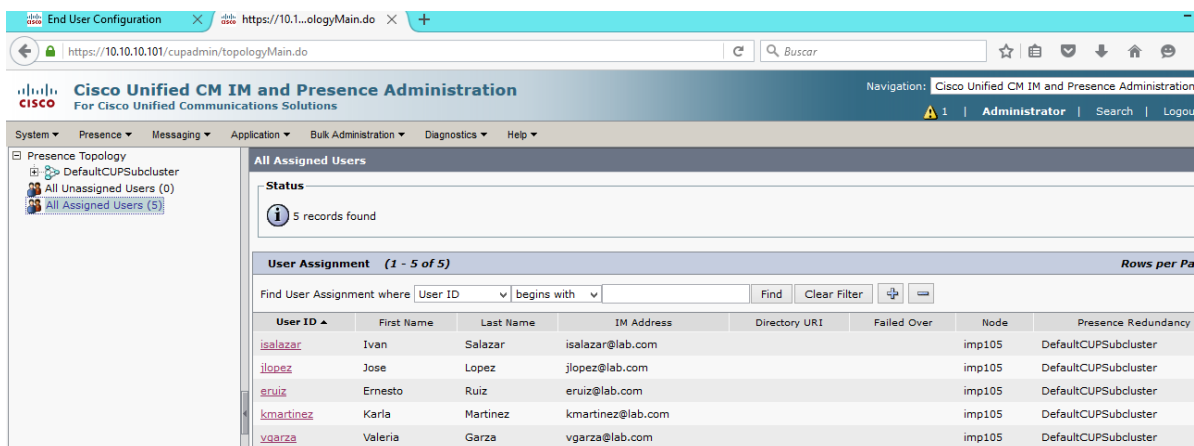
admin:utils sys
admin:utils system rest
admin:utils system restart

Do you really want to restart ?

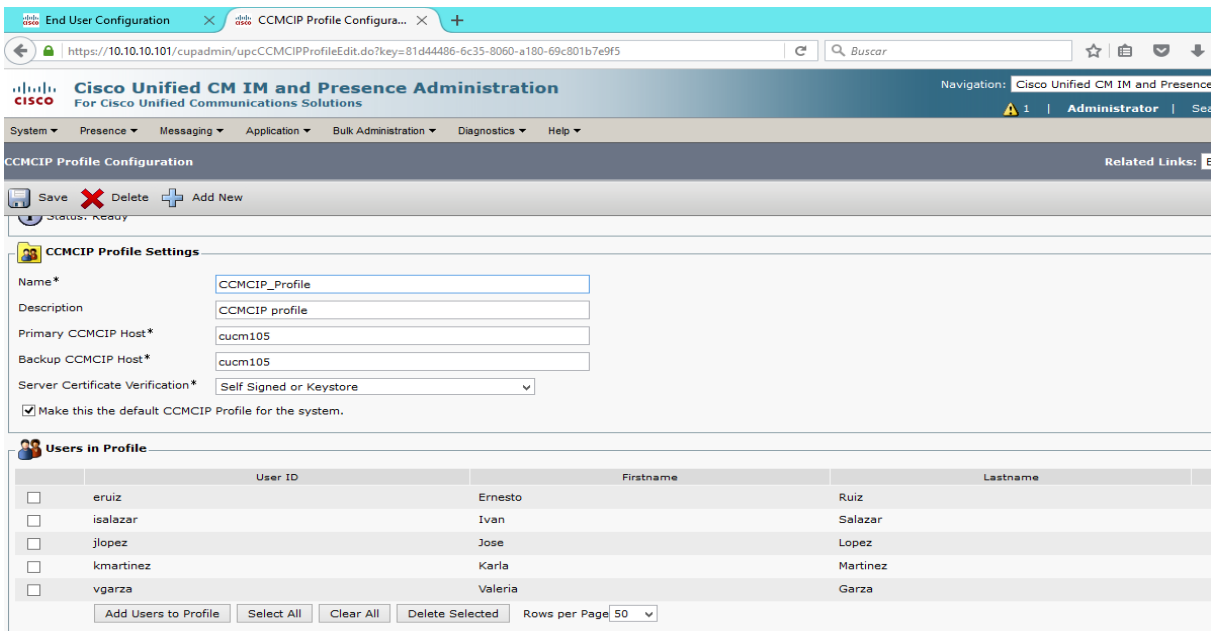
Enter (yes/no)? yes

Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
```

Una vez que reinicie, vemos que ya se activó el servicio de sincronización y ya vemos los usuarios sincronizados.



User ID	First Name	Last Name	IM Address	Directory URI	Failed Over	Node	Presence Redundancy
isalazar	Ivan	Salazar	isalazar@lab.com			imp105	DefaultCUPSSubcluster
jlopez	Jose	Lopez	jlopez@lab.com			imp105	DefaultCUPSSubcluster
er Ruiz	Ernesto	Ruiz	er Ruiz@lab.com			imp105	DefaultCUPSSubcluster
kmartinez	Karla	Martinez	kmartinez@lab.com			imp105	DefaultCUPSSubcluster
vgarza	Valeria	Garza	vgarza@lab.com			imp105	DefaultCUPSSubcluster



## Jabber Windows

Iniciamos la aplicación de Jabber una vez instalada en la computadora de un usuario en dominio, como está en dominio busca los servicios **SVR**, que configuramos en los DNS, lo unico que tenemos que hacer es poner el usuario y password del dominio.

