Configure Jabber for Windows - Quick Start Guide

Contents

Introduction

This document describes the necessary steps required for deployment of Cisco Jabber for Windows basic features.

Prerequisites

Cisco recommends you have a basic understanding of the Cisco Unified Communications Manager (CUCM) administration web page as well as experience with basic phone configurations.

Software Requirements

This guide assumes these software versions are in use:

- Cisco Unified Communications Manager (CUCM) version 10.x or higher
- Cisco Unified IM and Presence (IM&P) version 10.x or higher
- Cisco Unity Connection (CUXN) version 10.x or higher
- Jabber for Windows 11.8 or higher
- Microsoft Windows 10 (32 bit and 64 bit)
- Microsoft Windows 8 (32 bit and 64 bit)

- Microsoft Windows 7 Service Pack 1 or later (32 bit and 64 bit)

Hardware Requirements

The hardware specifications are the suggested minimum requirements for Cisco Jabber for Windows on a Microsoft operating system:

- CPU
  - Mobile AMD Sempron Processor 3600+ 2 GHz
  - Intel Core2 CPU T7400 at 2. 16 GHz
  - Intel Atom
- RAM
  - 2 GB (128 MB Free)
- Free Disk Space
  - 256 MB

Background

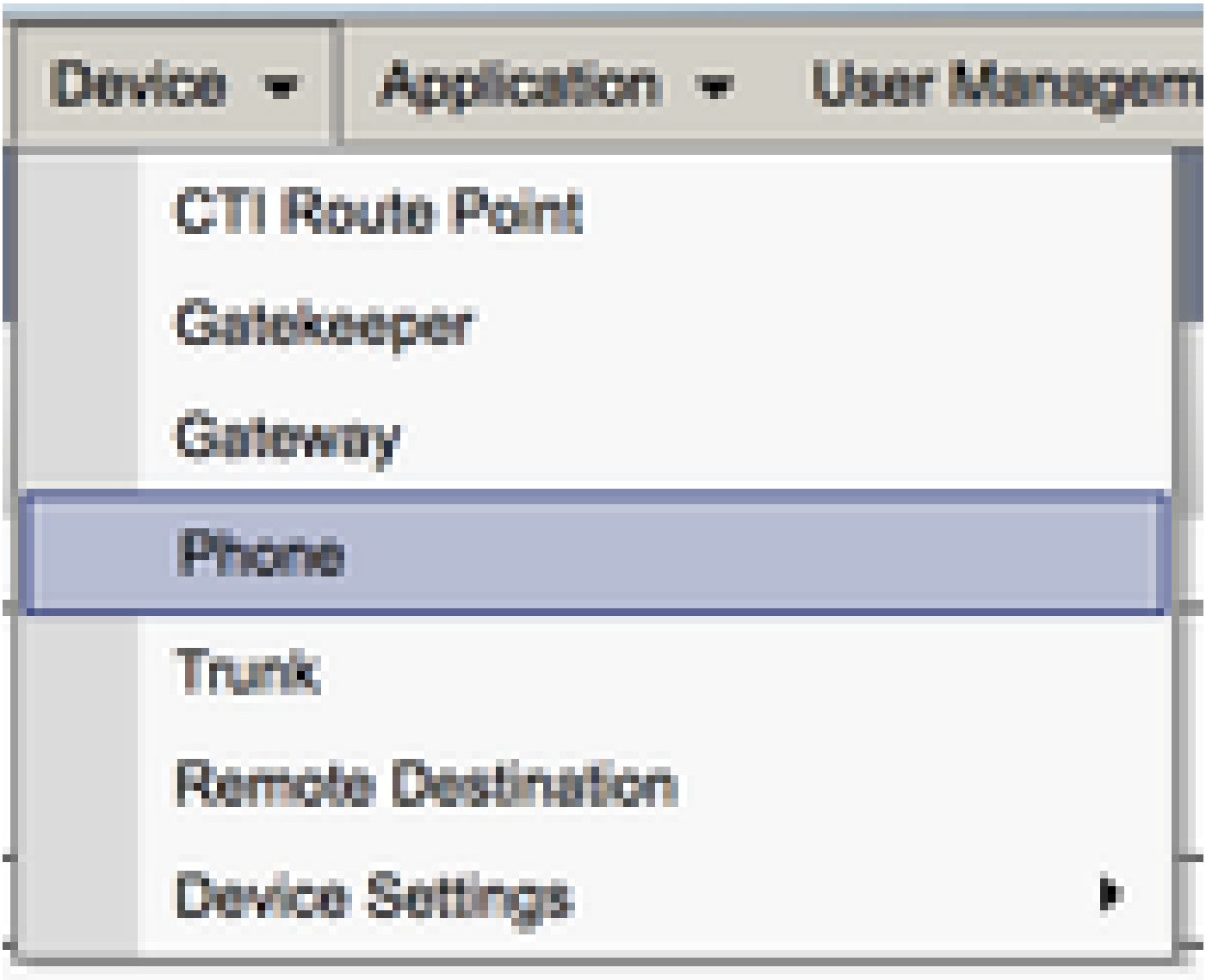
This is a quick start guide and does not cover any of the advanced features supported by Cisco Jabber for Windows.

Phone Services

Jabber Softphone

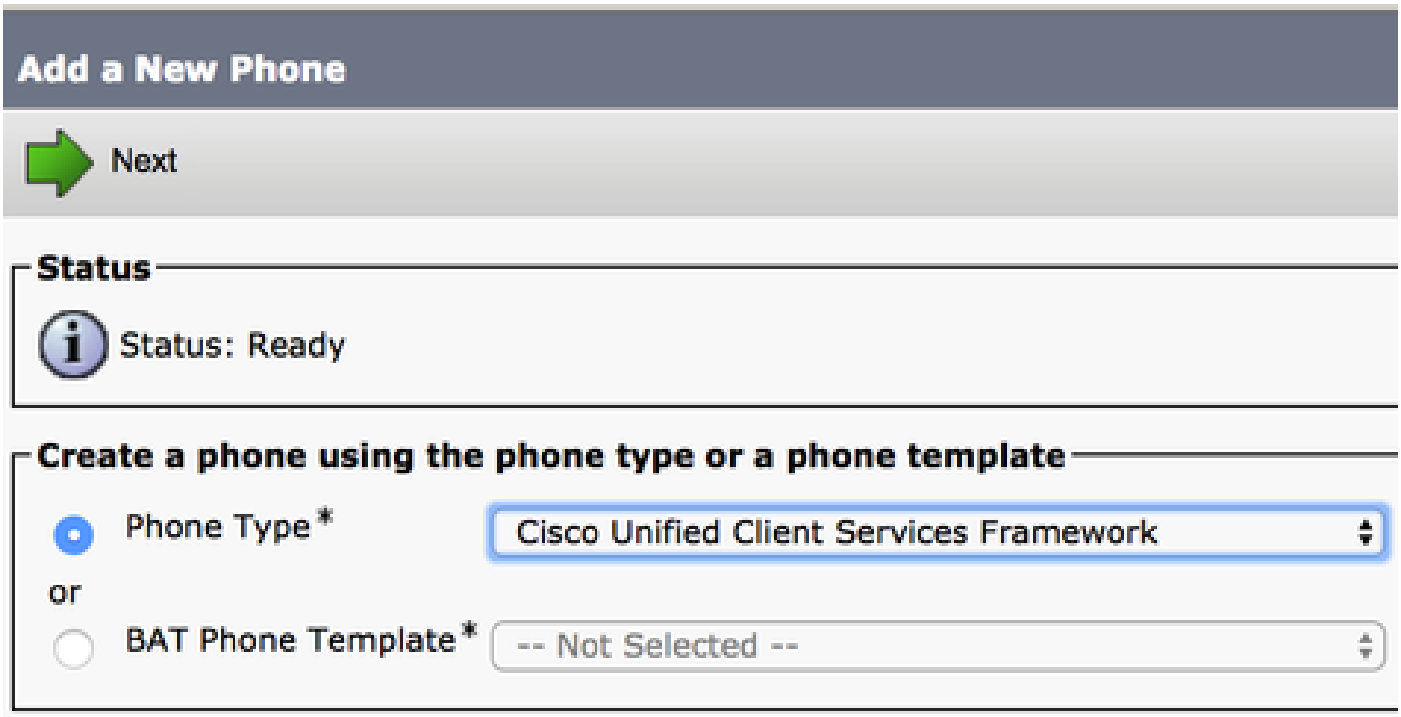
Jabber for Windows provides an option to supply phone services through a Cisco Unifed Client Services Framework devices which is often referred to as a CSF or Softphone.

To configure a CSF device, log into the CUCM Administration web page and navigate to **Device > Phone.**



From the **Find and List Phones** menu select **Add New.**

Once on the **Add a New Phone** menu, search the phone type drop down for the **Cisco Unifed Client Services Framework** device type. Once selected, click **Next**.



The table (Table 1.0) contains all the fields that must be configured to set up a Cisco Unified Client Services Framework (CSF) device in CUCM. The majority of required fields have default configurations which you do not need to manual configured unless otherwise required for your deployment. You must manually configure all the fields where the **Configured by Default** column in the table is set to **NO**.

> **Tip**: Cisco recommends that all Client Services Framework devices be configured with a device name prefix of CSF. For example, you provision a user named Holly Day with a CSF device. Her CUCM end user user ID is hday so her CSF device name would be CSFHDAY.

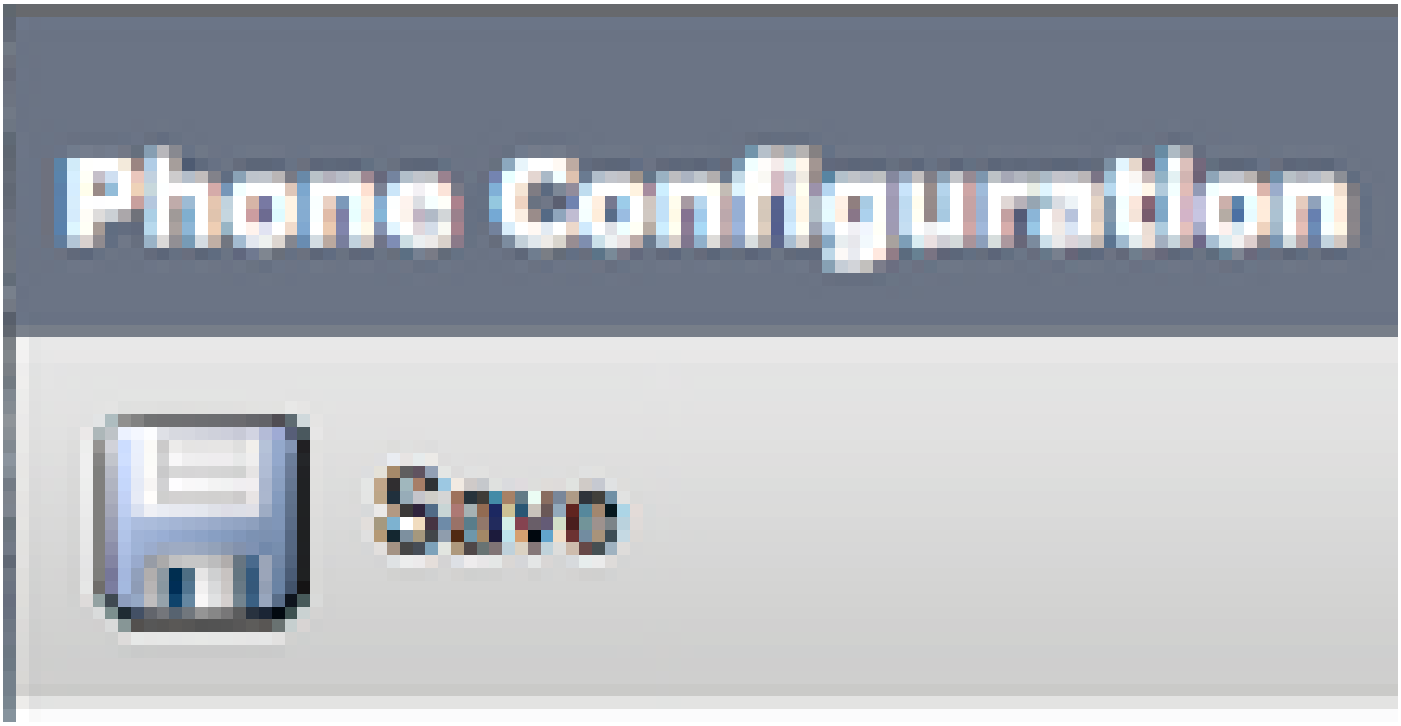
Table 1.0

Required Fields	Default Parameter	Configured by Default	Description
Device Name	Must be manually added, device name must begin with CSF	**NO**	Enter a name to identify software-based telephones
Device Pool	Must select one of the available device pools	**NO**	Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template.
Phone Button Template	Standard Client Service Framework	**NO**	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Common Phone Profile	Standard Common Phone Profile	YES	Choose a common phone profile from the list of available common phone profiles

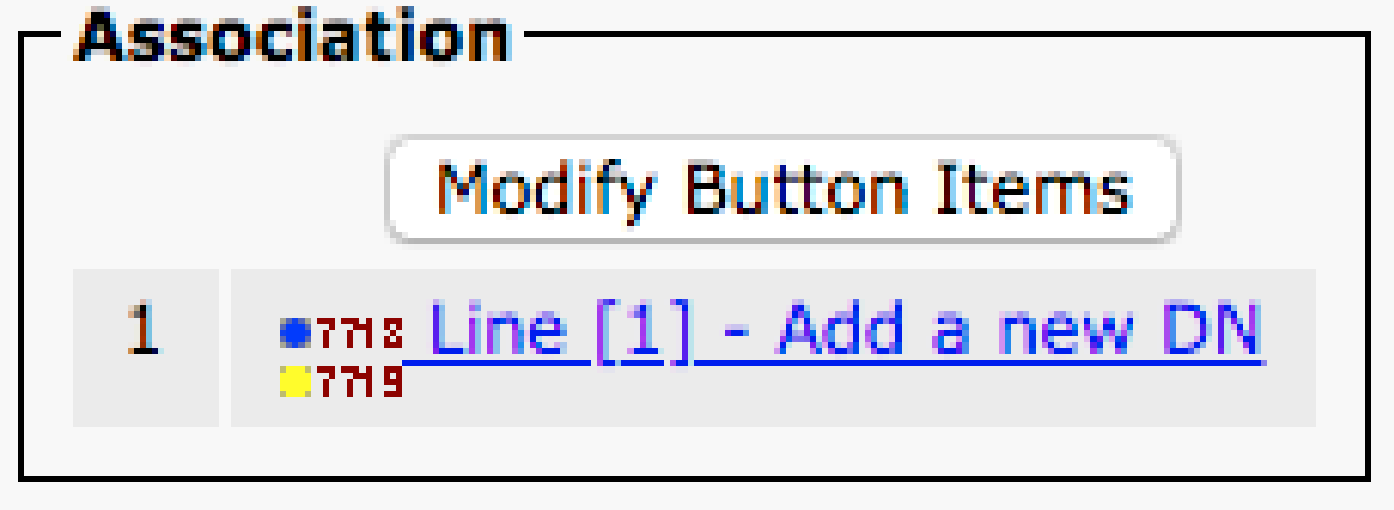
Location	Hub_None	YES	Use locations to implement call admission control (CAC) in a centralized call-processing system. The location specifies the total bandwidth that is available for calls to and from this location. A location of Hub_None means that the locations feature does not keep track of the bandwidth that this Cisco Unified IP Phone consumes. A location of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.
Built In Bridge	Default	YES	Enable or disable the built-in conference bridge for the barge feature with the Built In Bridge drop-down list box (choose On, Off, or Default)
Device Mobility Mode	Default	YES	Turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default uses the value for the Device Mobility Mode service parameter for the device.
Owner User ID	Set the user ID	**NO**	From the drop-down list box, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assign a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report.
Use Trusted Relay Point	Default	YES	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.
Always Use Primary Line	Default	YES	From the drop-down list box select (Off, On or Default). Default - Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	Default	YES	From the drop-down list box, select (Off, On or Default). Default - Cisco Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Packet Capture Mode	None	YES	This exists to troubeshoot encryption only; packet capturing can cause high CPU usage or call-processing interruptions.
BLF Presence Group	Standard Presence Group	YES	Choose a Presence group for the end user. The selected group specifies the devices, end users, and application users that can monitor this directory number. The default value for Presence Group specifies Standard Presence group, configured with installation.
Device Security Profle	Must be manually selected	**NO**	You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration. *Installing Cisco Unified Communications Manager*provides a set of predefined, nonsecure security profiles for auto-registration. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If

			the phone does not support security, choose a nonsecure profile.
SIP Profile	Must be manually selected	**NO**	Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.
Certificate Operation	No Pending Operation	YES	This field is related to CAPF enrollment.
DND Option	Ringer Off	YES	When you enable DND on the phone, this parameter allows you to specify how the DND features handle incoming calls.
Video Calling	Enabled	YES	Turns video capabilities on and off
Automatically Start in Phone Control	Disabled	YES	If enabled, start the client in desktop phone control mode.
Automatically Control Tethered Desk Phone	Disabled	YES	If enabled, the client automatically controls the tethered desktop phone.
Extend and Connect Capability	Enabled	YES	Indicates if Extend and Connect capabilities are enabled for the client. This allows the client to monitor and control calls on 3rd party PBX, PSTN, and other remote phones.
Display Contact Photos	Enabled	YES	Indicates if contact photo retrieval and display is enabled or disabled for the client.
Number Lookups on Directory	Enabled	YES	Indicates if phone number lookups with the Corporate Directory are enabled or disabled for the client.
Analytics Collection	Disabled	YES	Indicates if analytics collection is enabled or disabled for the client.

Once you have configured all the required fields for the CSF configuration, save the configuration with the **Save** button.



Now that you have created a CSF, you need to add a directory number to the device. This can be done by selecting the **Add a new DN** option located at the top left of the CSF configuration.



Note: This document does not cover the complete line configuration for the CSF device. Line configuration is a standard configuration that must be performed for all phones and is not a configuration that is specific to CSF devices.

Tip: Once you have a directory, number your CSF device make sure to associate the CUCM end user to the directory number. Scroll to the bottom of the directory number configuration and **Associate End Users**. This configuration is required if you plan to use Jabber for phone presence.

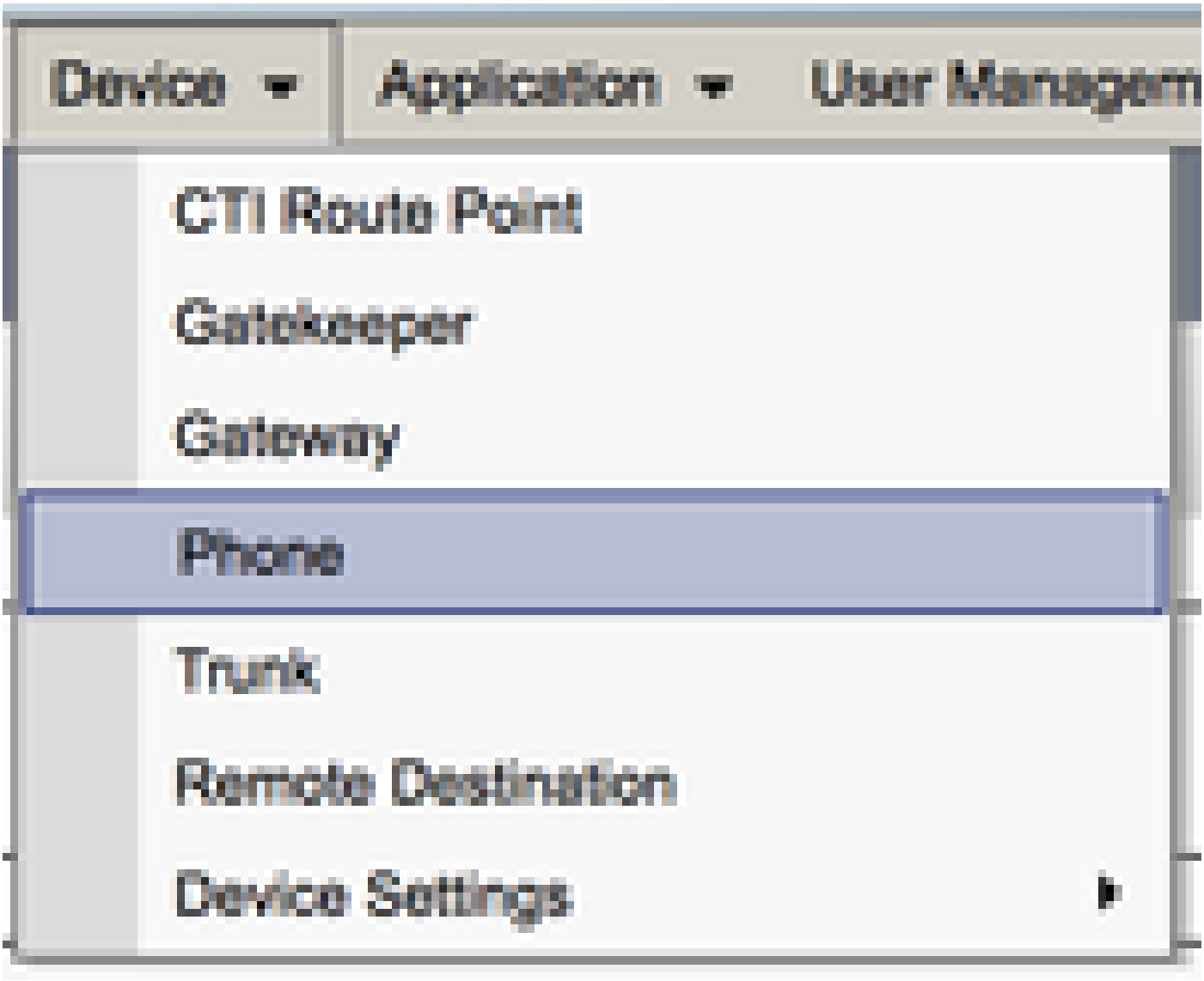
Jabber Deskphone

Jabber for Windows also has the capability to perform Cisco Computer Telephony Integration (CTI) with Cisco deskphones. This allows Jabber for Windows users to use their Cisco deskphone as their Jabber telephony device when perform call actions from the Jabber user interface.

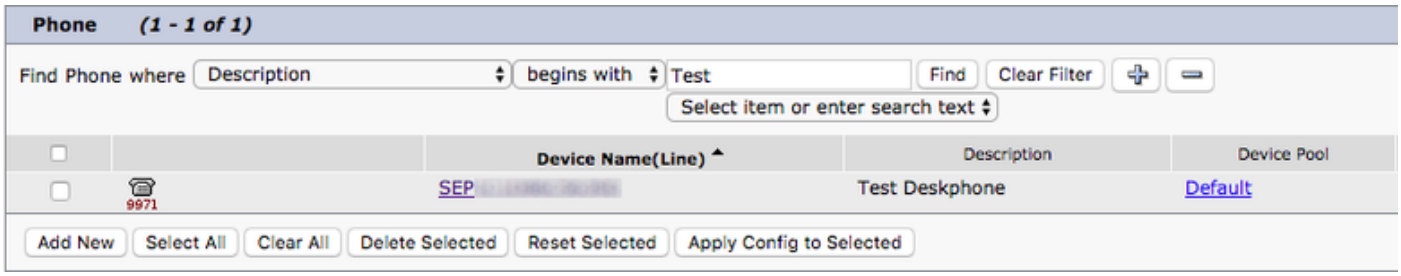
Deskphone Configuration

To setup Jabber for Windows CTI integration, complete these steps:

Access the CUCM Administration web page and navigate to **Device > Phone.**



From the **Find and List Phones** menu, search for and select the Jabber users deskphone.

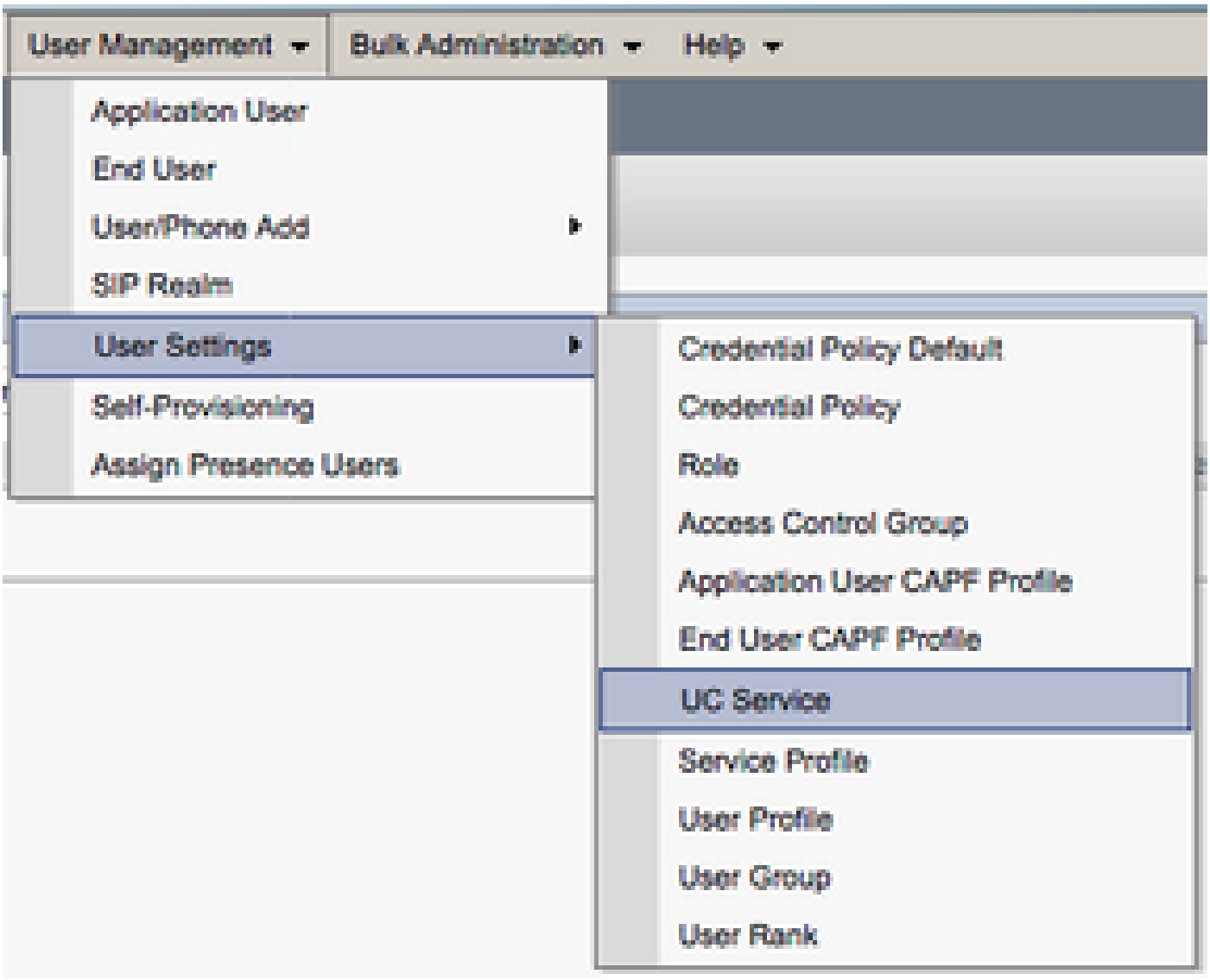


When presented with the **Phone Configuration** menu, verify the two listed:

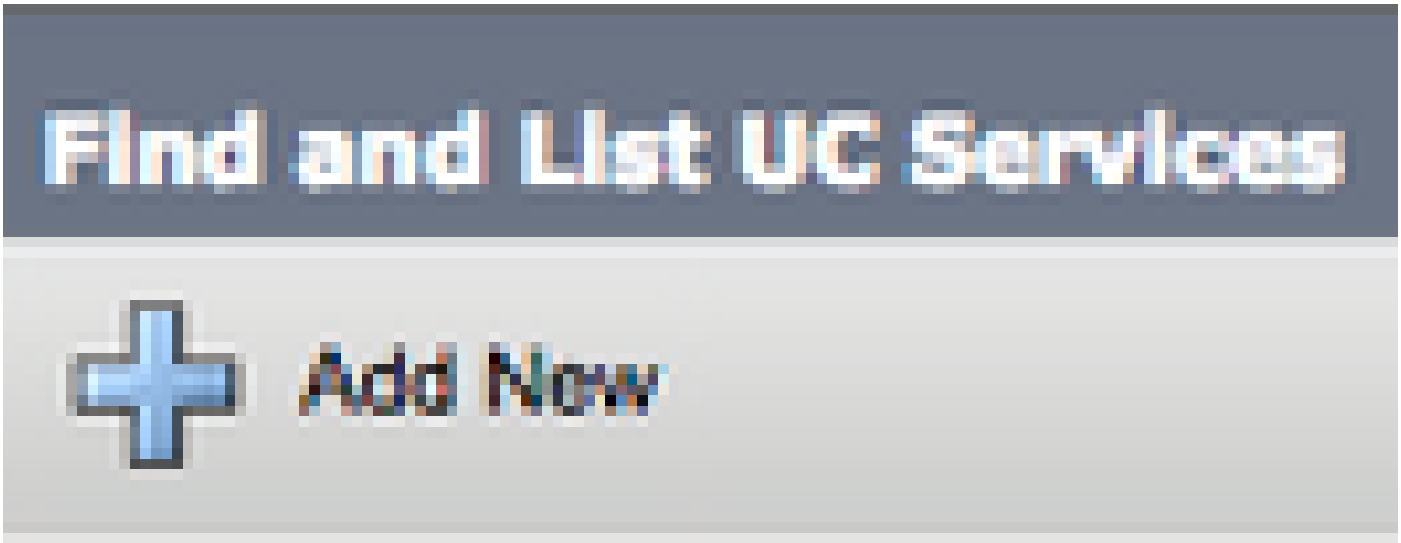
1. Verify that the **Allow Control of Device from CTI** check box is checked.
2. Confirm the device **Owner User ID** is set to the Jabber for Windows user CUCM user ID.

CTI UC Services Setup

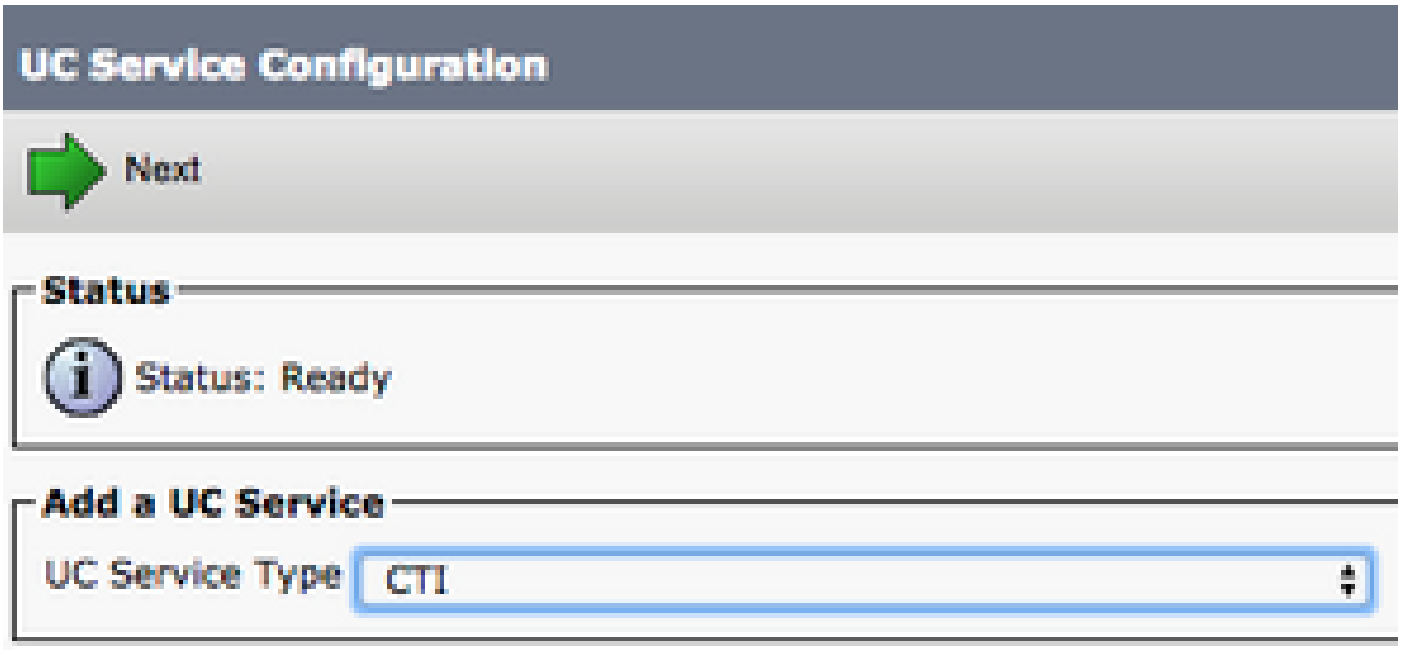
Next we setup the CTI UC services that is to be used by the Jabber client to connect to the CUCM CTIManager service. Navigate to **User Management > User Settings > UC Service.**



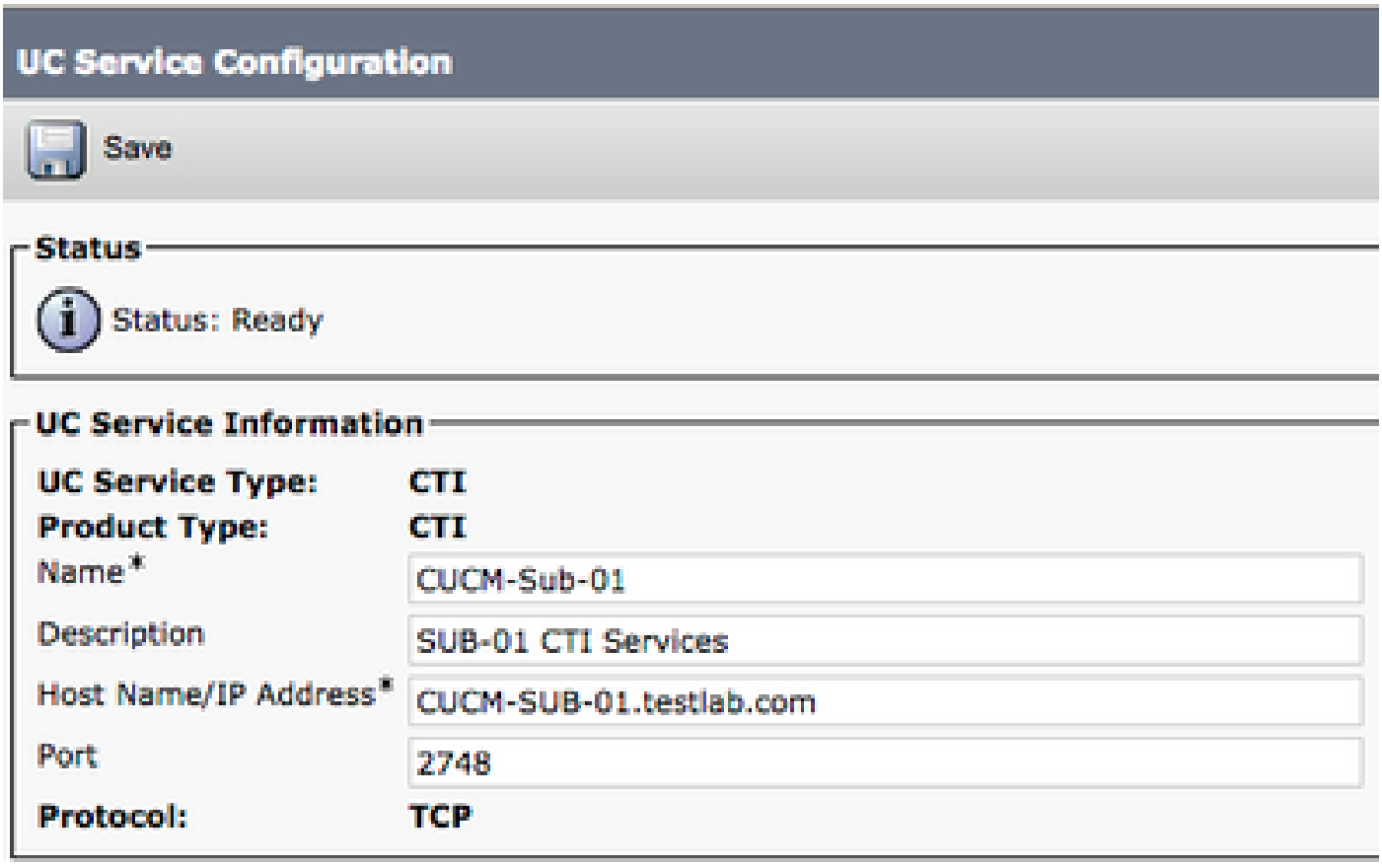
Once on the **Find and List UC Services** page, select **Add New**.



When presented with the **UC Service Configuration** page, select **CTI** from the **UC Service Type** drop down then select **Next**.

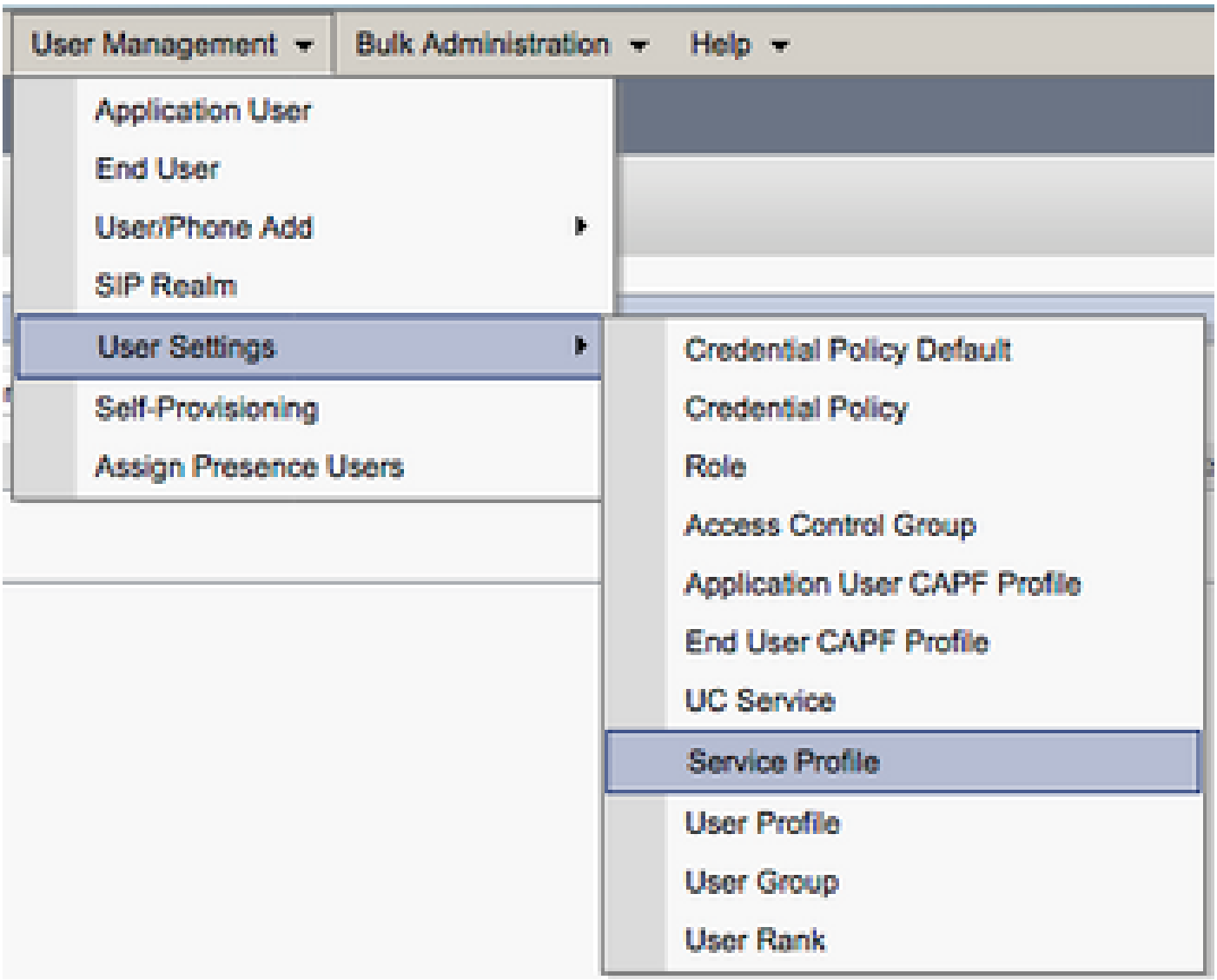


Then, you are presented with the **UC Service Configuration** page. Here configure a **Name** for the CTI UC Service as well as provided the **IP, Hostname or Fully Qualified Domain Name (FQDN)** of the CUCM server that has the CTI service active.



Note: Up to three CTI UC Services can be assigned to a UC Service Profile.

Now that we have defined the CTI UC Service(s), we assign them to the Service Profile. Navigate to **User Management > User Settings > Service Profile**.



From the **Find and LIst Service Profiles** menu, search for and select the service profile used by your Jabber for Windows users or create a new service profile with **Add New**.

This document does not cover the configuration of a new new Cisco deskphone as this is a basic CUCM administration task.

To view the list of (CTI) supported devices, navigate to **CUCM Cisco Unified Reporting** and select the **Unified CM Phone Feature List Report**. Next select **CTI controlled** from the Feature drop-down list.

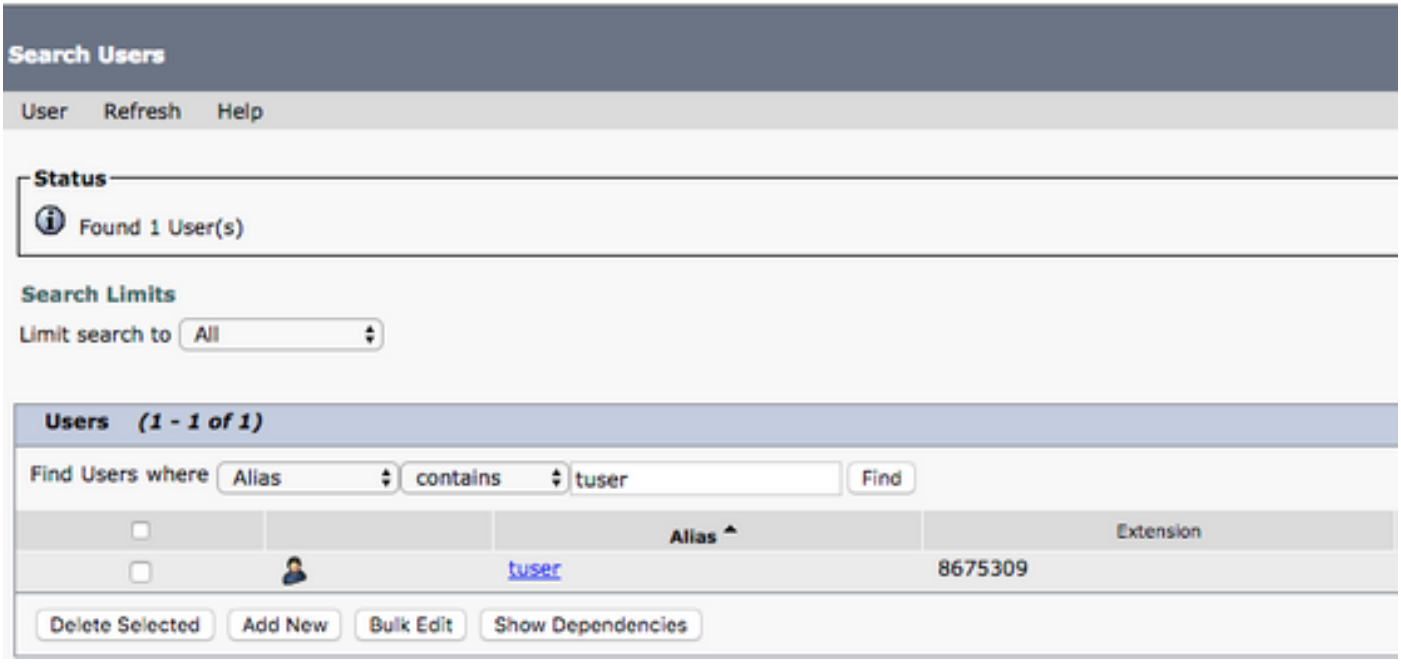
Configuration of the Voicemail

Jabber for Windows is able to retrieve and playback voicemail messages that have been stored on Cisco Unity Connection. To setup voicemail for Jabber for Windows, complete these steps:

Unity Connection Configuration

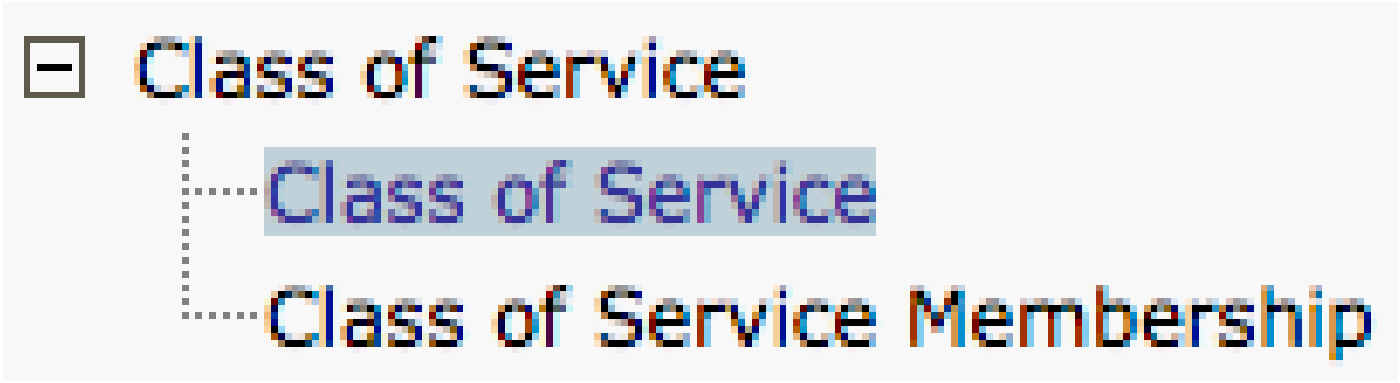
Access the Cisco Unity Connection web administration web page and navigate to **Users > Users.**

When presented with **Search Users** page, search for and select your Jabber for Windows users mailbox.

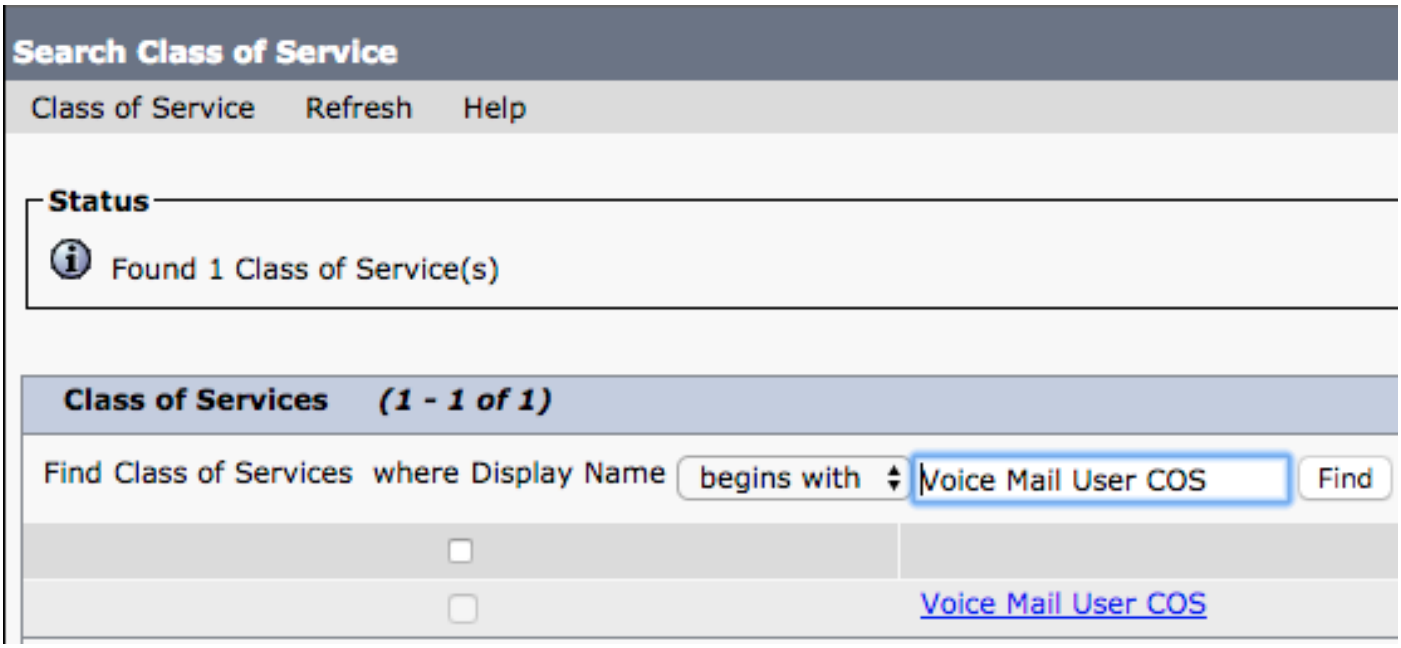


Once presented with the **Edit User Basics** page of the user Mailbox, notate the **Calls of Service** that is configured.

Via the left hand navigation pane, navigate to **Class of Service > Class of Service.**



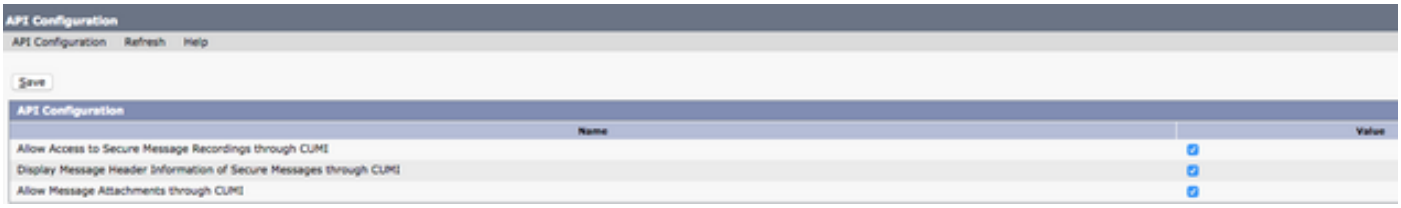
When presented with the **Search Class of Service** page, search for and select the class of service you previously notated.



Once on the **Edit Class of Service** page, verify:

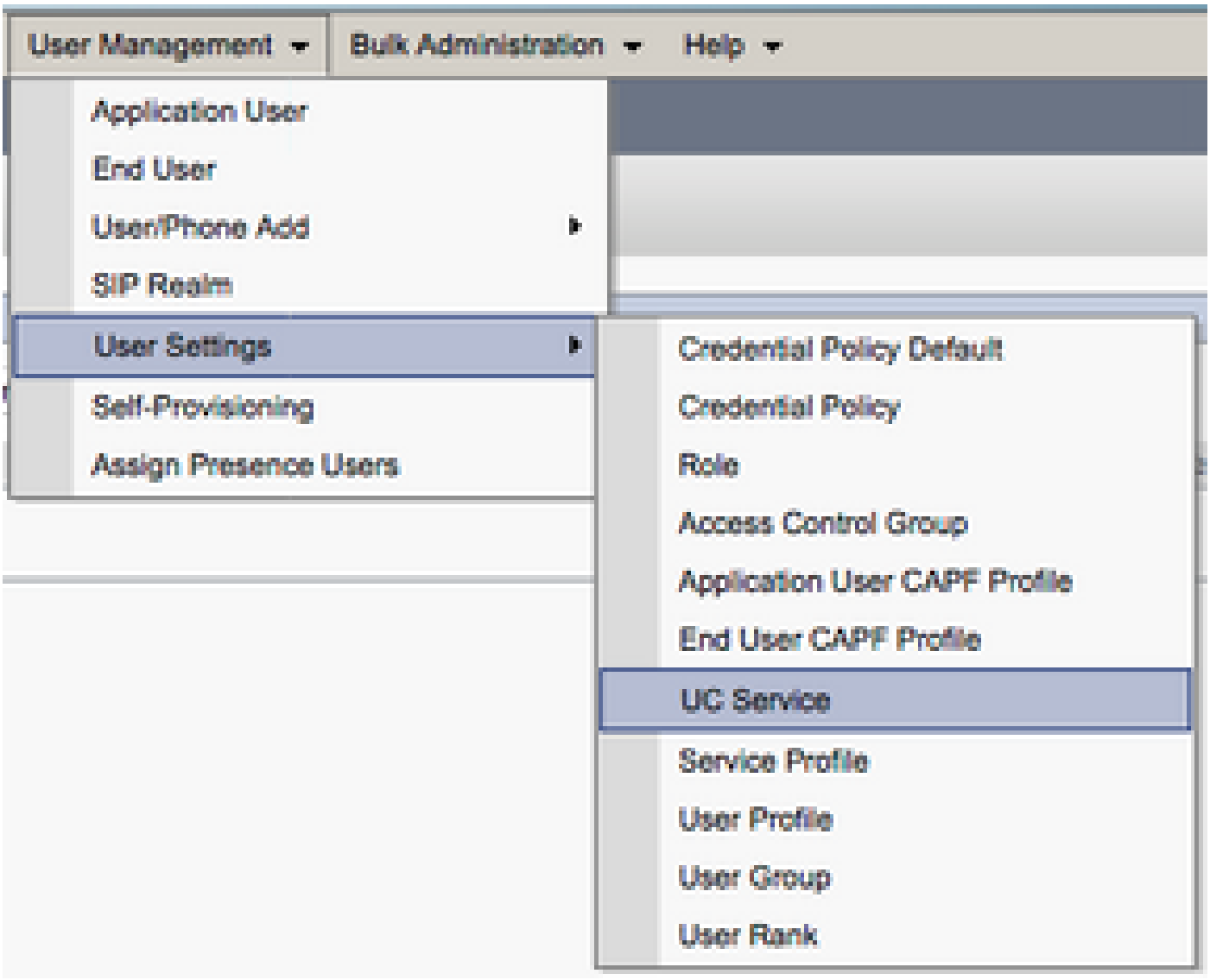
1. The check box is checked for the **Allow Users to Use the Web Inbox and RSS Feeds** feature.
2. The **Allow Users to Use Unified Client to Access Voicemail** feature is enabled by the box near the feature name.

Once the Class of Service configuration has been verified, navigate to **System Settings > Advanced > API Settings** in the left navigation pane. Enable all three presented on the **API Configuration** page.

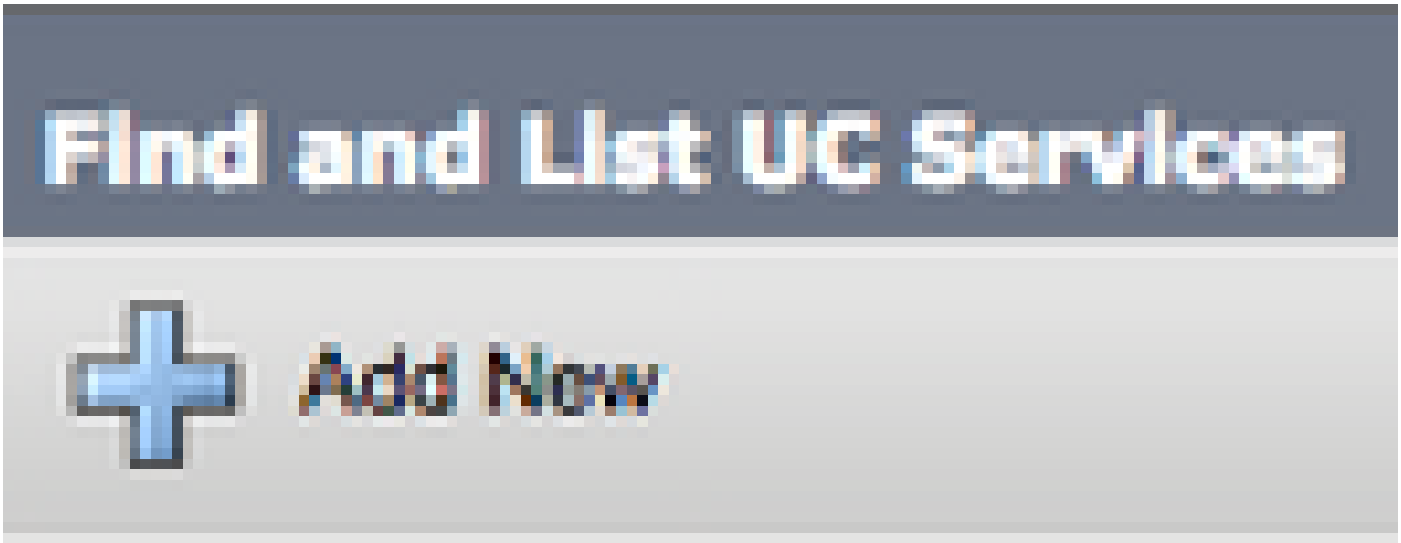


CUCM Configuration

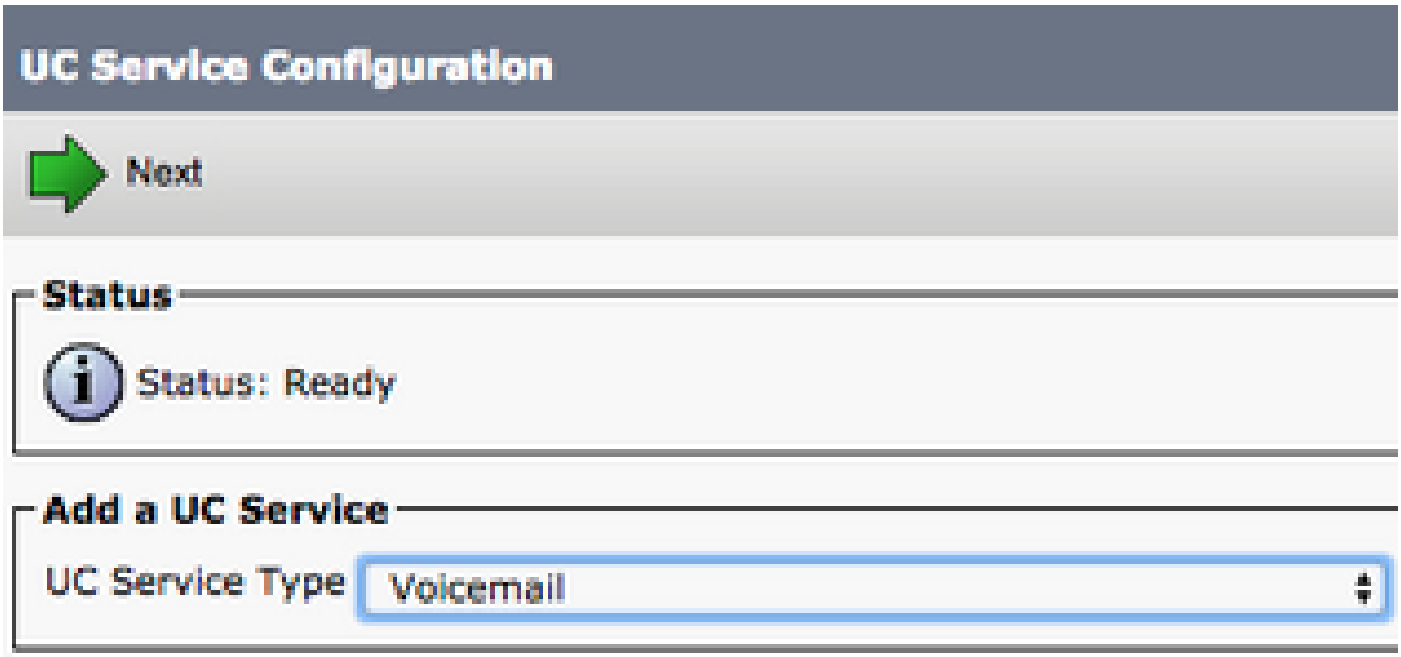
Now that Unity Connection is setup, we move to the CUCM configuration for Jabber for Windows voicemail. Navigate to **User Management > User Settings > UC Service.**



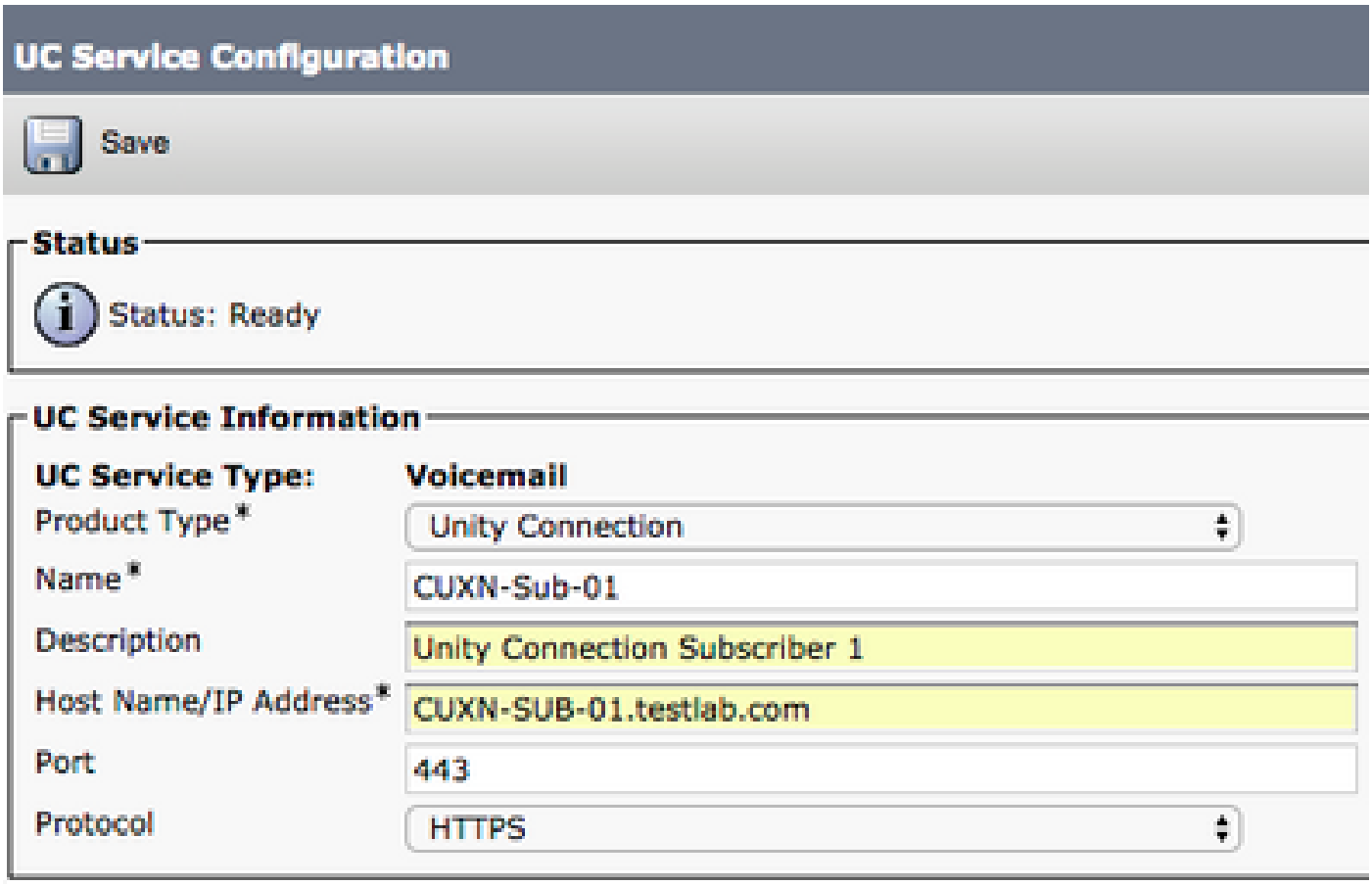
Once on the **Find and List UC Services** page, select **Add New**.



When presented with the **UC Service Configuration** page, select **Voicemail** from the **UC Service Type** drop down then select **Next**.



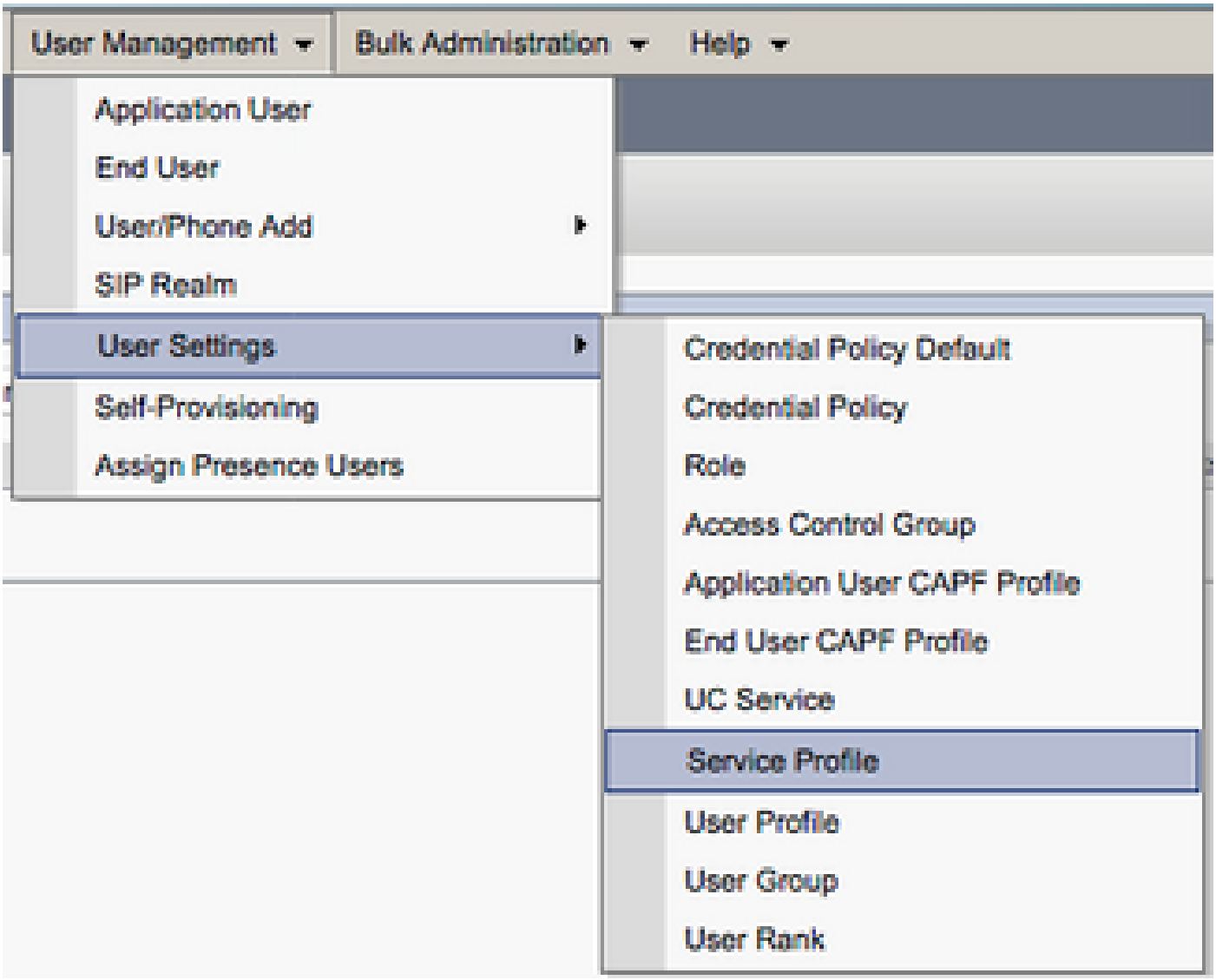
Once presented with the **UC Service Configuration** page, select **Unity Connection** from the **Product Type** dropdown. We need to configure a **Name** for the VoicemailUCService as well as provide the**IP, Hostname or Fully Qualified Domain Name (FQDN)** of the Unity Connectionserver that acts as the REST and Jettyservices.



Note: Up to three VoicemailUCServices can be assigned to aUCService Profile.

Now that the Voicemail UC Service(s) are defined, we assign them to the Service Profile. Navigate to **User**

Management > User Settings > Service Profile.



From the **Find and LIst Service Profiles** menu, search for and select the service profile used by your Jabber for Windows users or create a new service profile with **Add New**.

: The Jabber for Windows setup assumes that Unity Connection is LDAP authentication. In cases where mailboxes are not LDAP integrated, please refer to the Cisco On-Premises Deployment Guide.

Configuration of the Directory

Jabber for Windows is dependent on directory services for resolution of corporate contacts. Jabber is able to perform directory resolution through Lightweight Directory Access Protocol (LDAP) or CUCM User Data Services (UDS). Please refer to the next sections for information on configuration of LDAP or UDS directory services for Jabber for Windows.

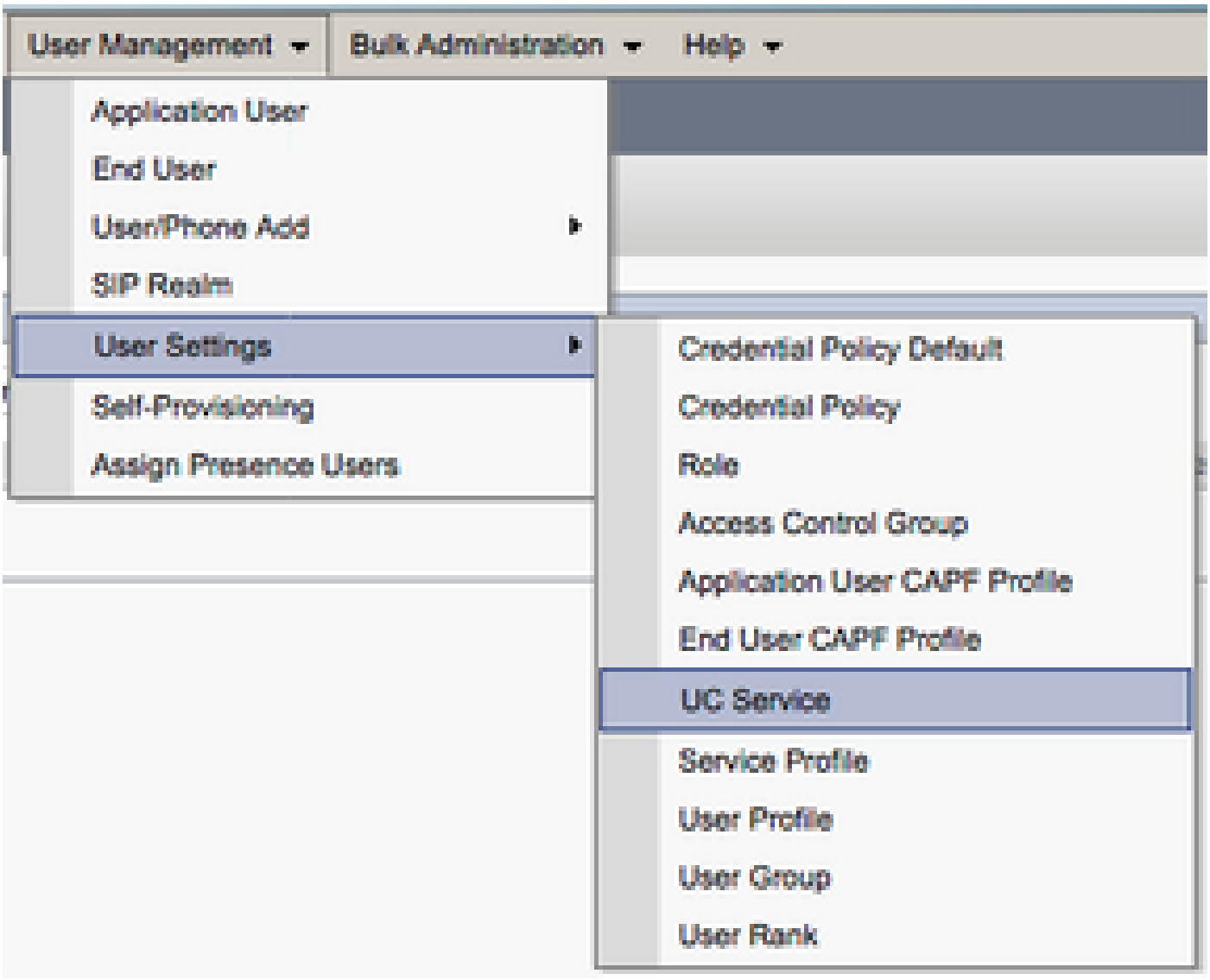
LDAP Directory Services

Jabber for Windows supports three well known LDAP directory services:

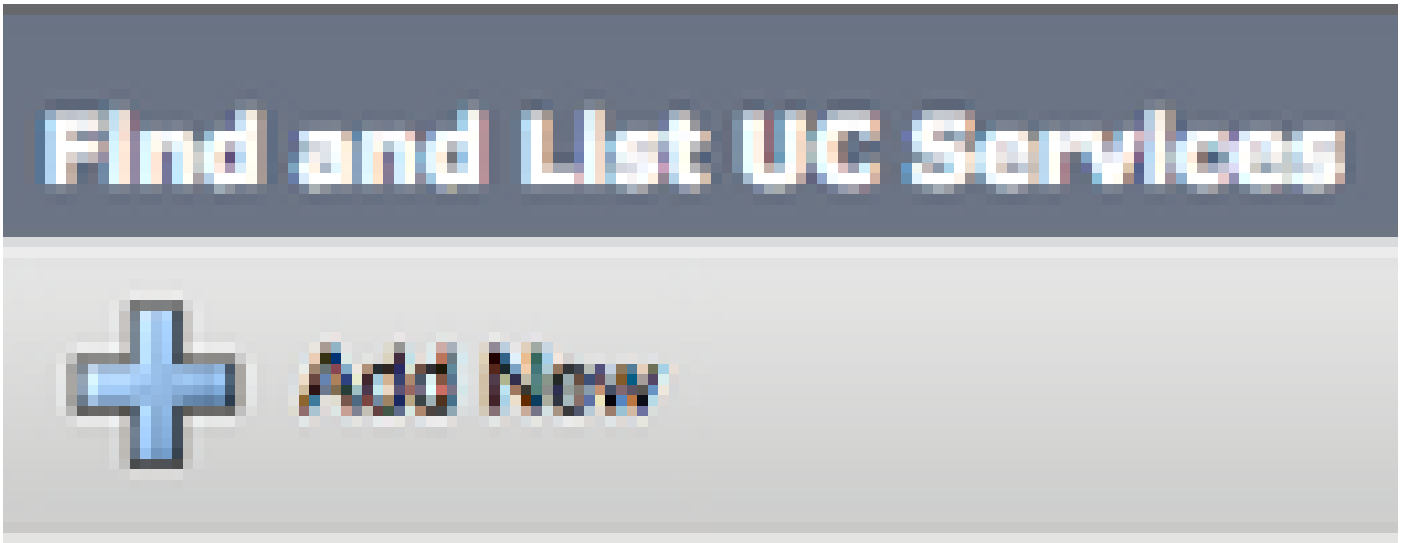
- Active Directory Domain Services
- OpenLDAP
- Active Directory Lightweight Directory Service (AD LDS)

This guide provide the steps to configure Jabber for Windows 11.8 or higher to integrate with Active Directory Domain Services, as this is the most common integration.

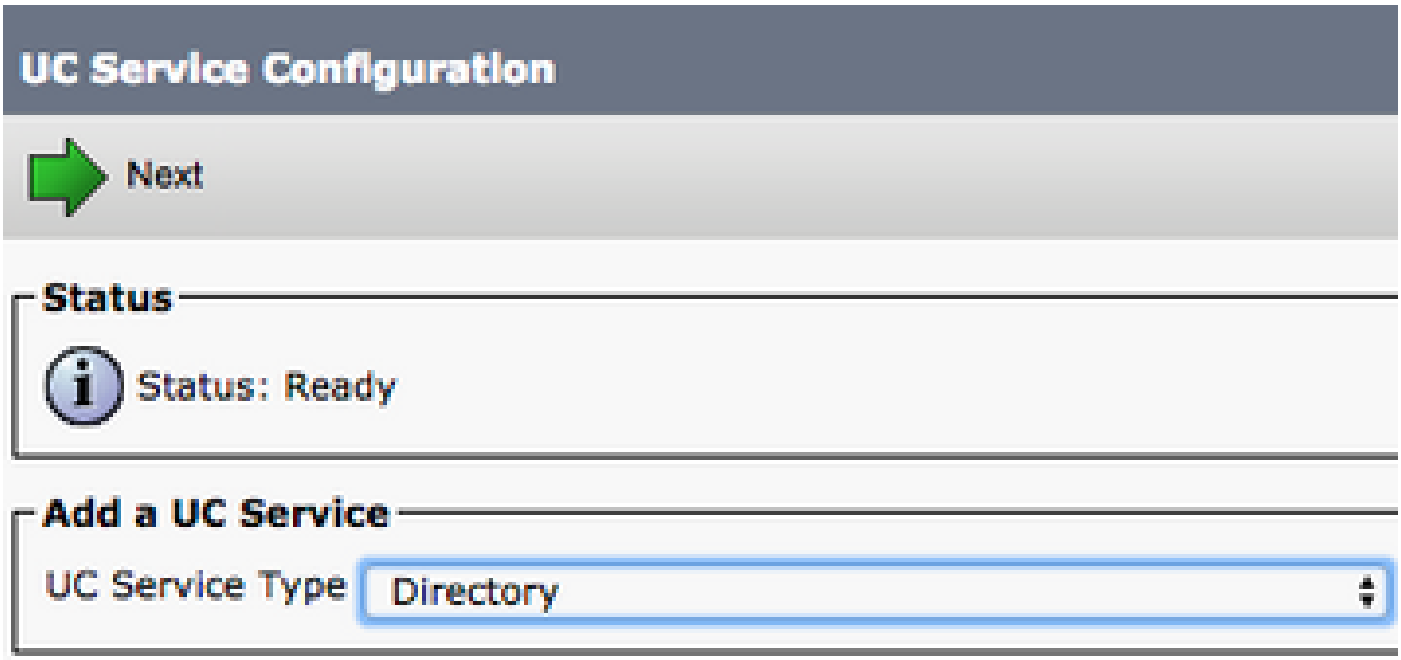
Access the CUCM Administration web page and navigate to **User Management > User Settings > UC Service**.



Once on the **Find and List UC Services** page, select **Add New**.



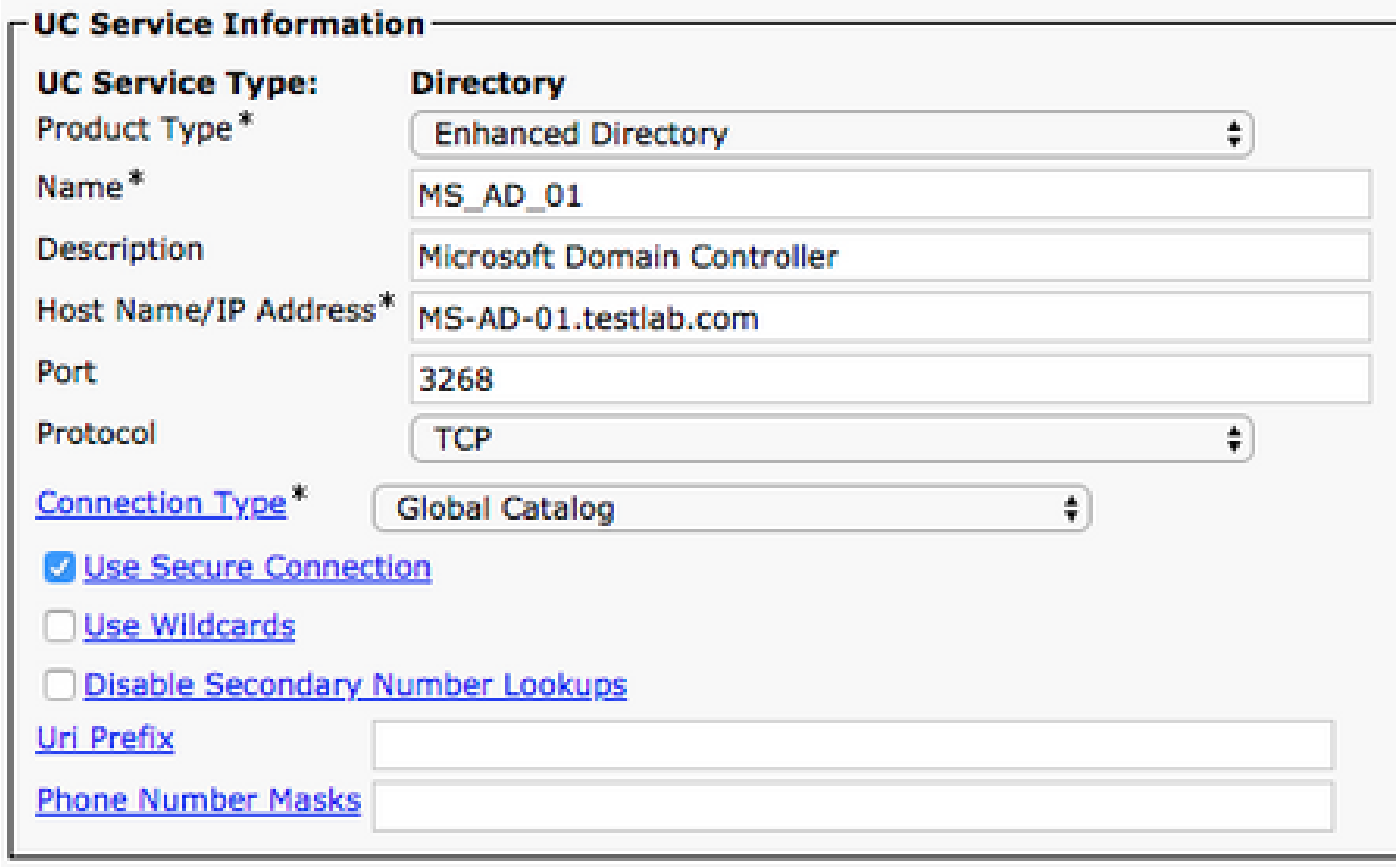
When presented with the **UC Service Configuration** page, select the **Directory** from the **UC Service Type** drop down and select **Next**.



On the **UC Service Configuration** page, select **Enhanced Directory** from the **Product Type** drop down. You also need to configure a **Name** for the Directory UCService as well as provided the**IP, Hostname or Fully Qualified Domain Name (FQDN)** of the directory server.

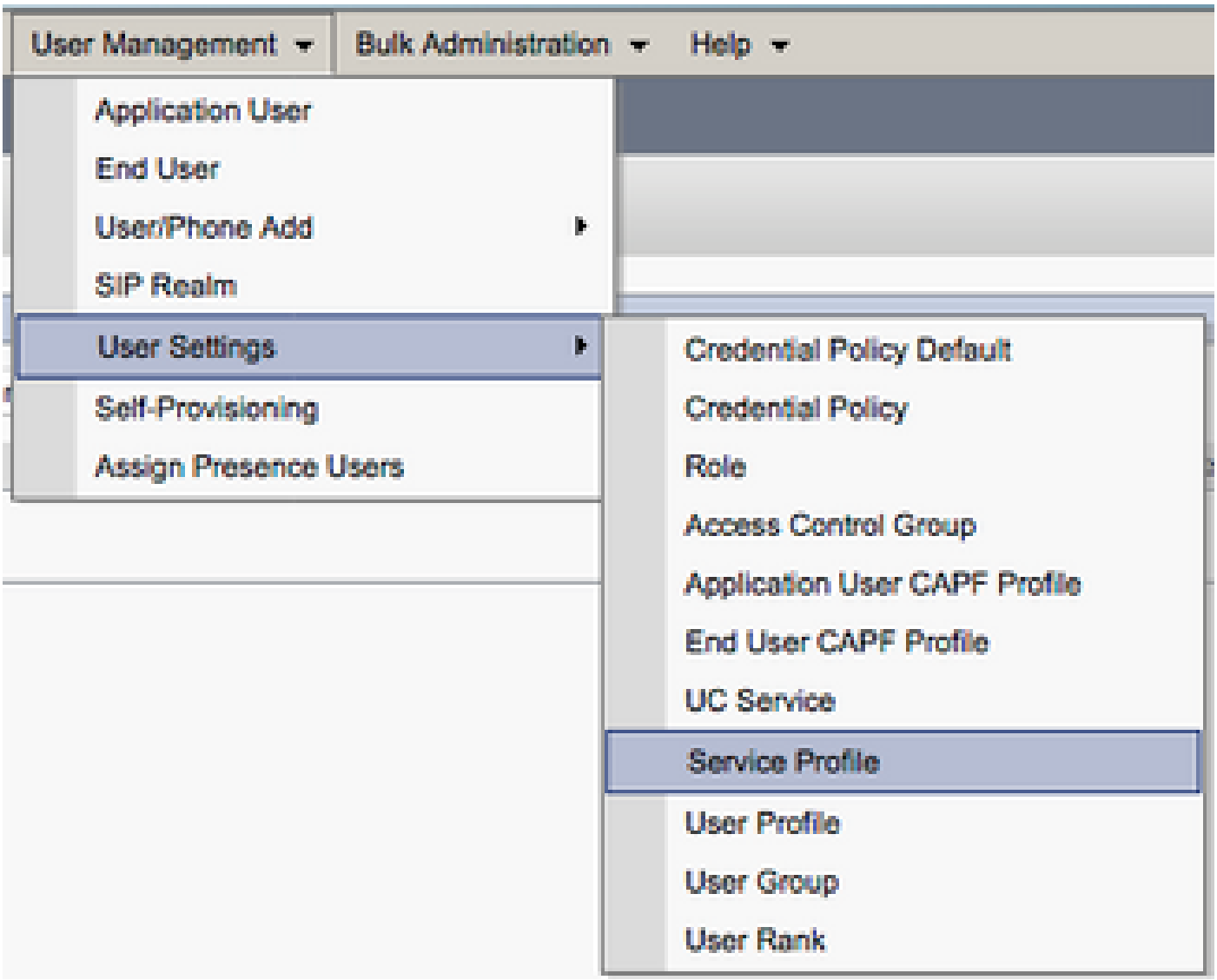
By default the **Connection Type** is set to **Global Catalog** which assumes that a Microsoft Domain Controller is used as the the directory source. If a Global Catalog server is in use, the **Port** number in the configuration must be set to **3268**. Cisco does recommend the use of a Global Catalog server as a directory resource as it provides more efficient resolutions of queries.

> **Tip**: In cases where you do not have a domain controller for Microsoft Active Directory Domain Services, the Directory UC Service must have the **Port** set to **389** to **Connection Type** must be set to **Ldap**.



Note: Up to three DirectoryUCServices can be assigned to aUCService Profile.

Now that the Directory UC Service(s) are defined, we assign them to the Service Profile. Navigate to **User Management > User Settings > Service Profile**.



From the **Find and LIst Service Profiles** menu, search for and select the service profile used by your Jabber for Windows users or create a new service profile with **Add New**.

UCService(s) to the service profile. You also need to define the Active Directory search base, this can be the organization unit or directory where your corporate users exist.

While in the **Directory Profile** section, you also have to configure a directory authentication method. Check the check box near the "**Use Logged On User Credential**" to prevent anonymous queries and force Jabber to authenticate with the credentials that were entered during Jabber log in. If the **Use Logged On User Credential** is left unchecked, Jabber can attempt to perform anonymous access to the directory server. Anonymous directory access is not recommended by Cisco.

Once you are done with the **Directory Profile**, select **Save**.

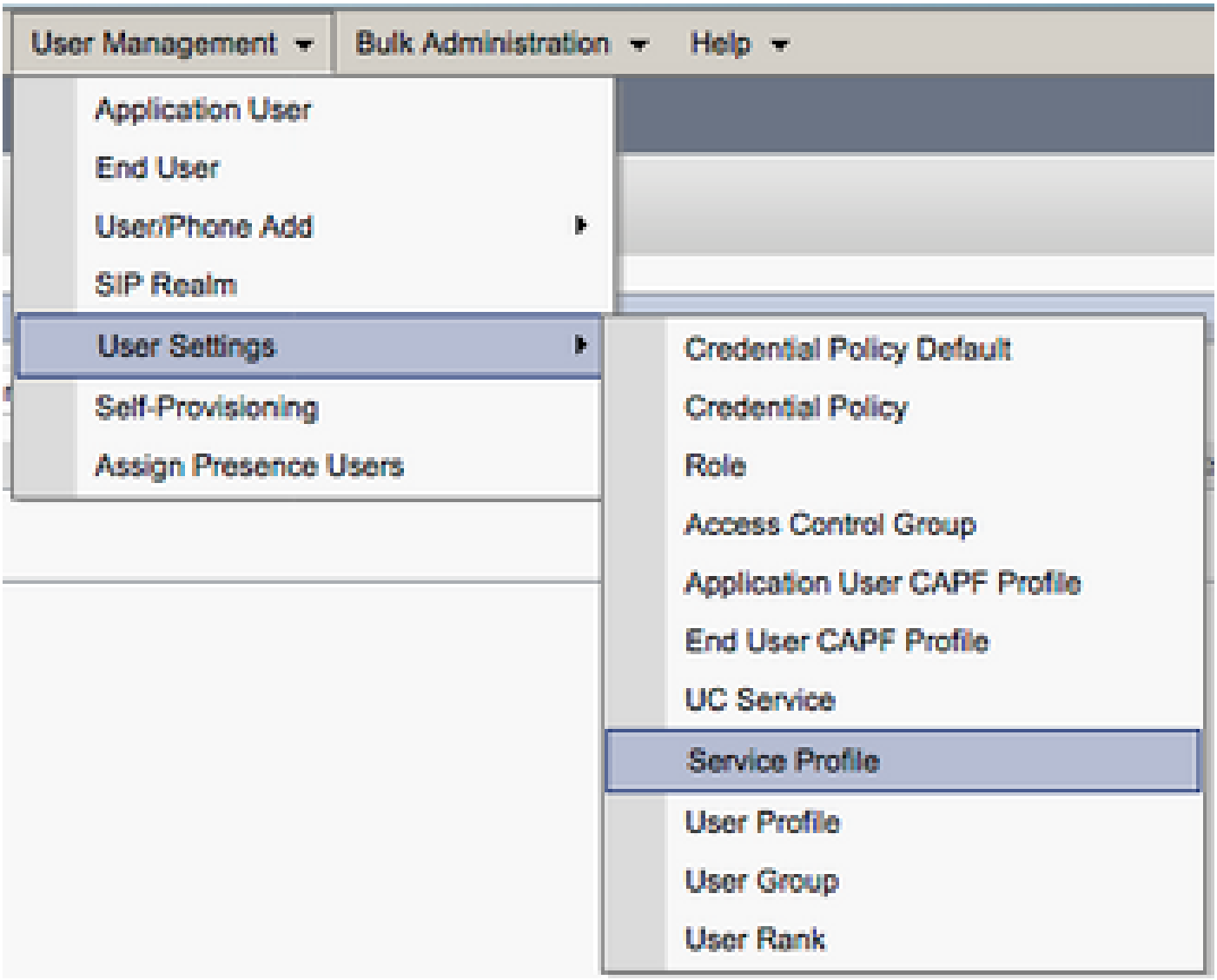
> **Note**: If you are in CUCM 10.X - 11.5.X, the Directory Profile section of the Service Profile also include username and password fields that allow for a distinguished name to be used as the user ID that is authorized to run queries on the LDAP server. In CUCM 12.X, if you want to use a single user ID for authentication for directory services, you need to use the ConnectionUsername and ConnectionPassword parameters in the jabber-config.xml.

> **Caution**: Cisco Jabber queries contact source with various attributes. Not all of these attributes are indexed by default. To ensure efficient searches the attributes used by Cisco Jabber must be indexed on the directory server. For more information please refer to the LDAP Prerequisites section of the Jabber Planning Guide.

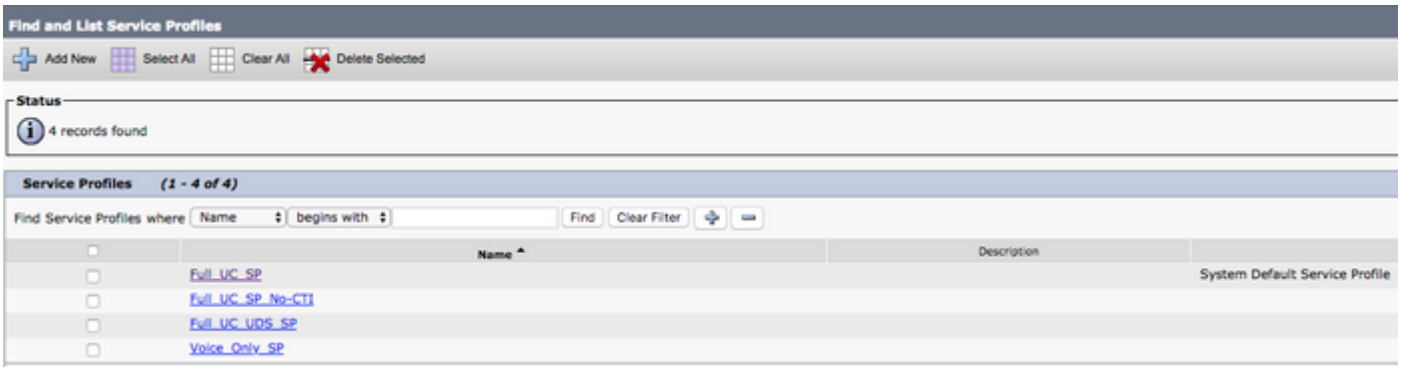
UDS Directory Services

CUCM User Data Services (UDS) provides a contact source API that can be used by Jabber over Cisco Expressway mobile and remote access for the contact resolution, and it is an optional contact service for clients on the corporate network. The UDS contact source uses the Unified CM end user table information to provide a directory resolution.

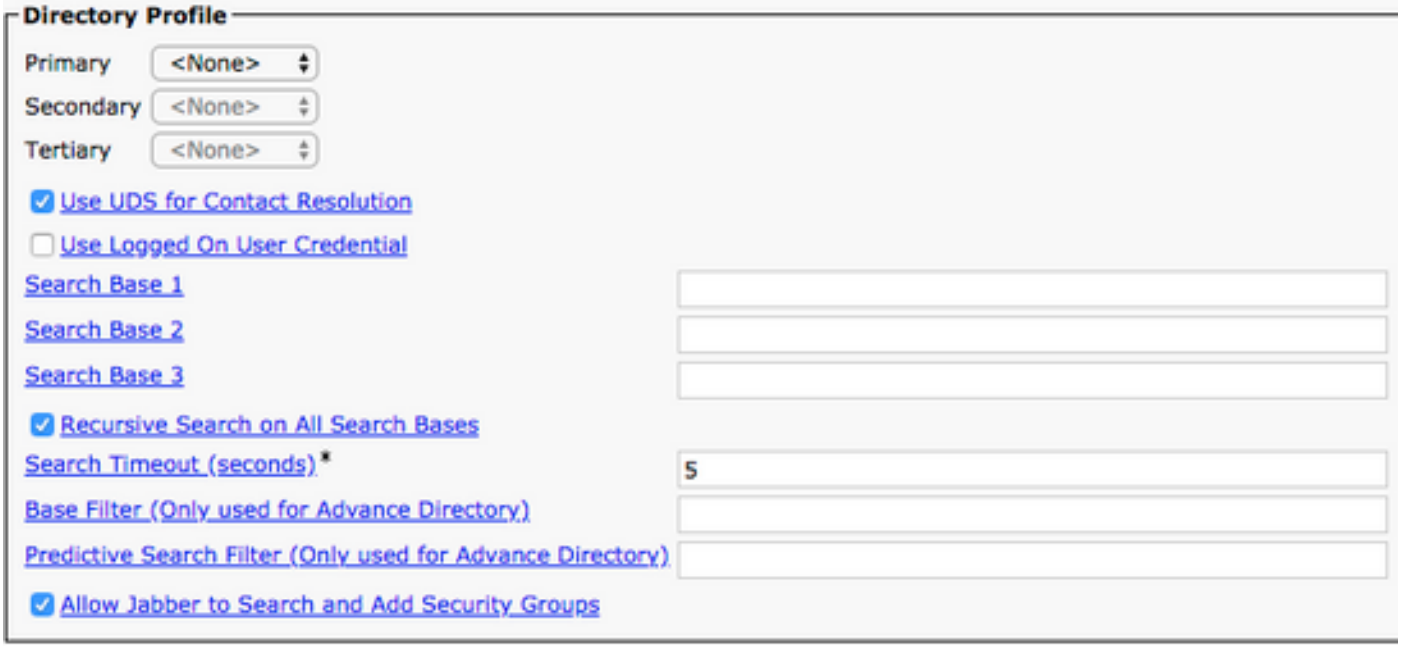
Access the CUCM Administration web page and navigate to **User Management > User Settings > Service Profile**.



From the **Find and LIst Service Profiles** menu, search for and select the service profile used by your Jabber for Windows users or create a new service profile with **Add New.**



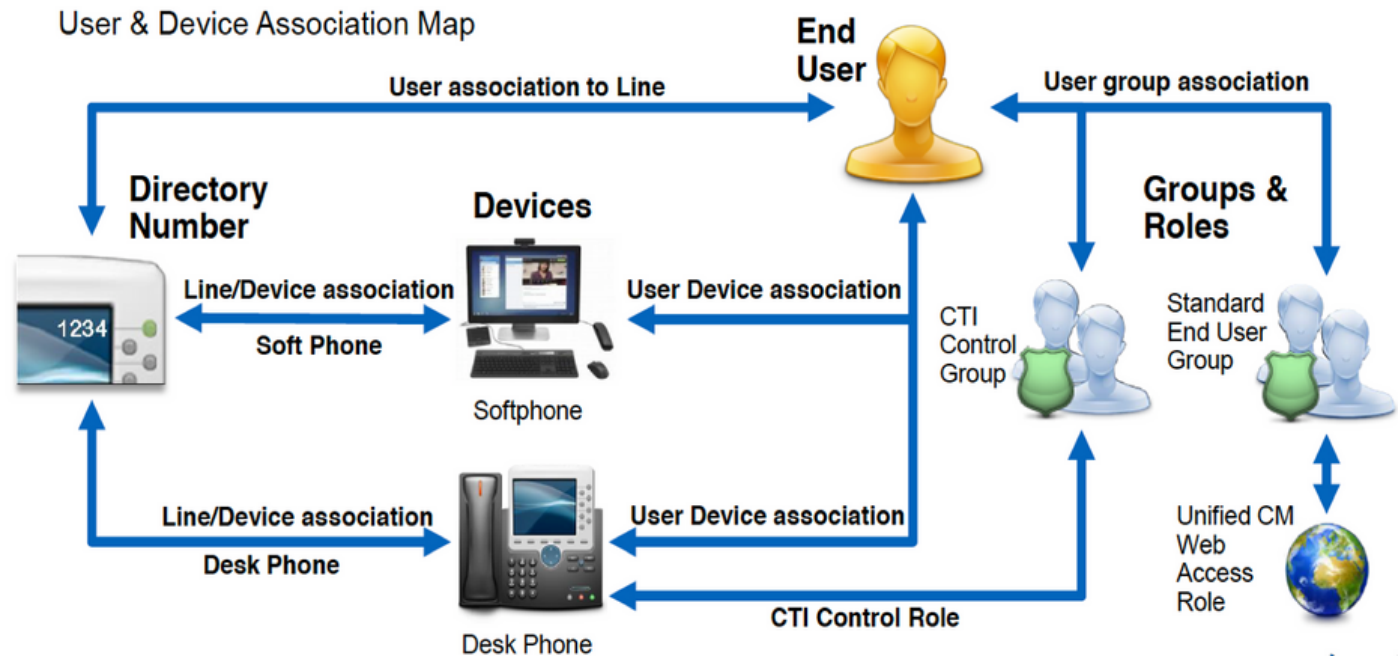
Once on the **Service Profile Configuration** page, scroll down to the**DirectoryProfile** section and check the check box labeled **Use UDS for Contact Resolution** then select **Save.**



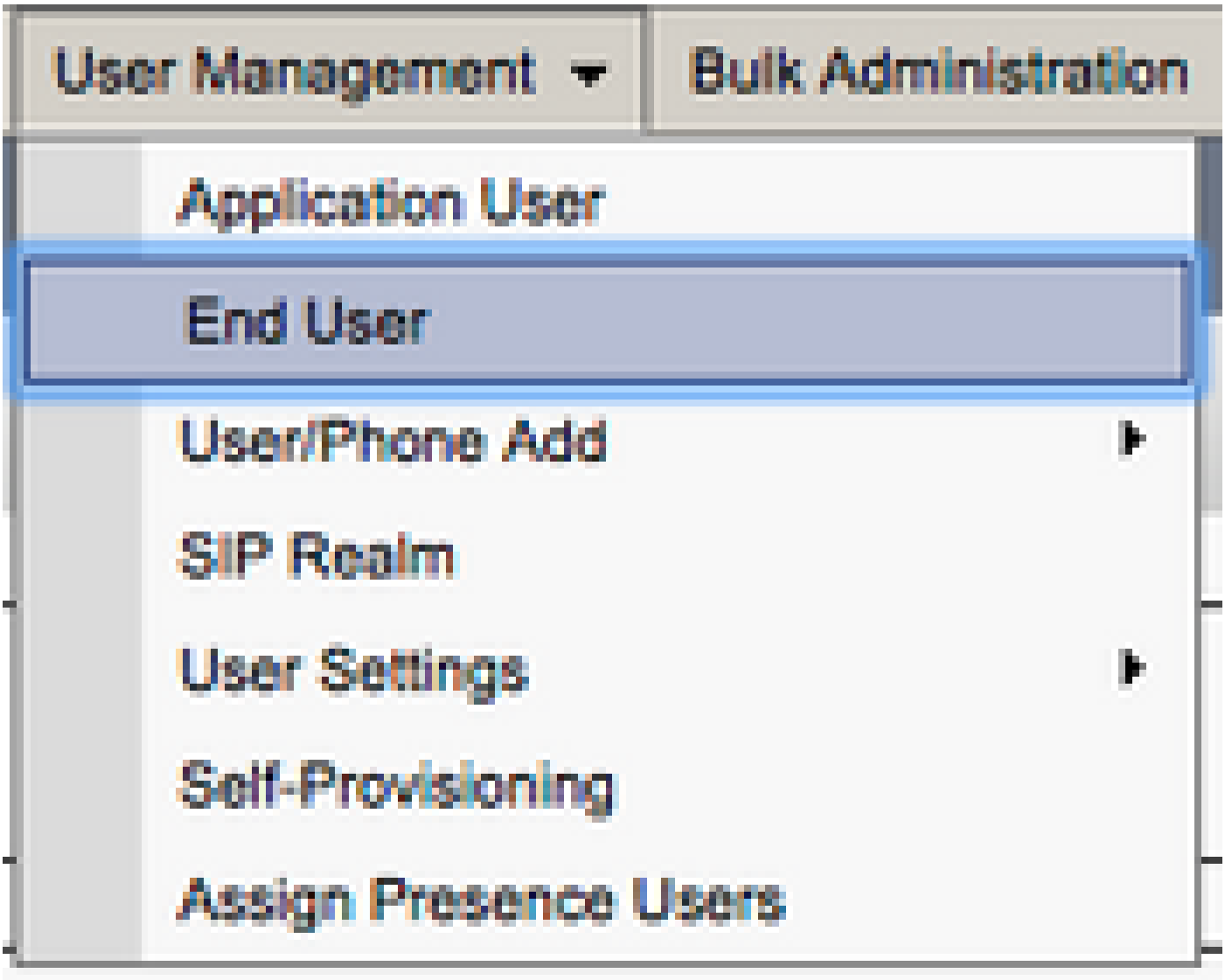
Once UDS Is enabled on the service profile, Jabber for Windows automatically discovers the CUCM UDS servers during the Jabber log in process.

Configuration of the CUCM End Users

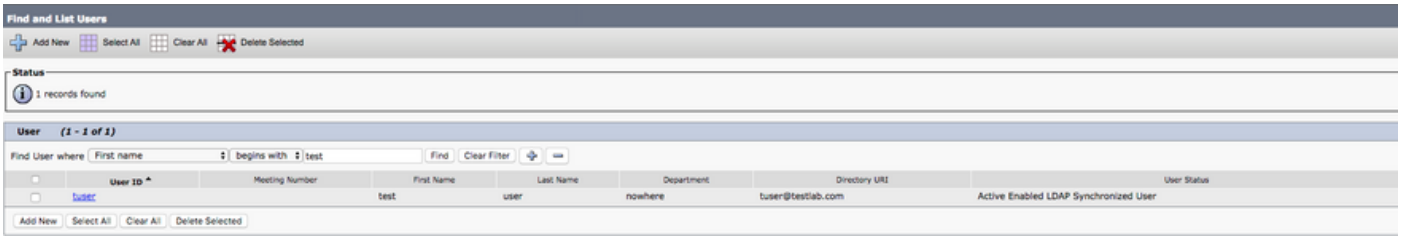
The CUCM end user configuration is a crucial step for Jabber for Windows as many of Jabbers features are dependent on this configuration. The image depicts all the Jabber configurations that are dependent on the CUCM end user configuration.



To configure the Jabber for Windows CUCM end user, acess the CUCM Administration web page and navigate to **User Management > End User**.



From the **Find and LIst Users** menu, search for and select the CUCM end user you wish to configure for Jabber for Windows.



Once on the **End User Configuration** web page, scroll down to the **Service Settings** section. Here you can assign the end user the services you want them to use. To enable a user to be able to log in to Jabber for Windows, you must enable the **Home Cluste**r service by the check box next to the service name.

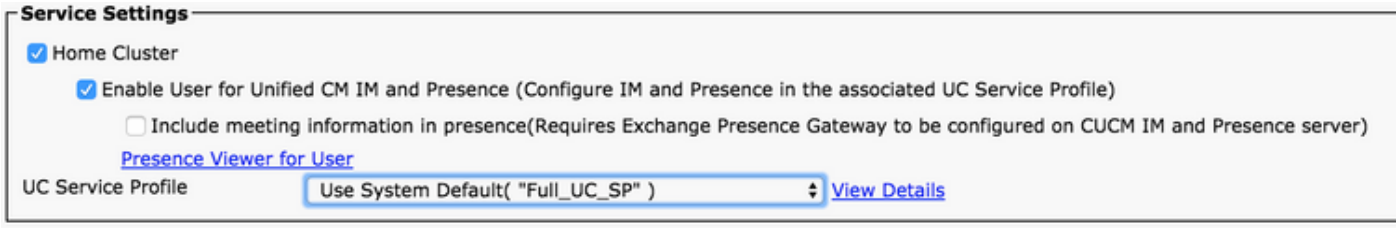
If your end is target to use Jabber for Windows for instant messaging, you need to enable their end user for the service by the check box next to the field labeled **Enable User for Unified IM and Presence.**

Next you want to assign a service profile with a service profile from the **UC Service Profile** drop down. The service profile is used to provide the Jabber client with CUCM UC service configuration. .

Note: If you do not assign a service profile to the CUCM end user then the user automatically, use the

---

service profile that is set as the system default service profile.



Next scroll down to the **Device Information** section. Here you can manage the CUCM end users controlled devices. Assign the user their softphone and/or deskphone devices. CUCM provides this list of device to Jabber for Windows during Jabber log in.

You can assign a device to a user with the **Device Association** button. You are presented with the **User Device Association** menu. From here you can search for the CUCM end users devices. When you find a device place a check mark in the check box next to the device and select **Save Selected Changes**.

Now scroll down to the **Directory Number Association** section and select the CUCM end users primary extension from the **Primary Extension** drop down.

Scroll down to the **Permissions Information** section. Here we assign the permissions that are needed by Jabber for Windows.

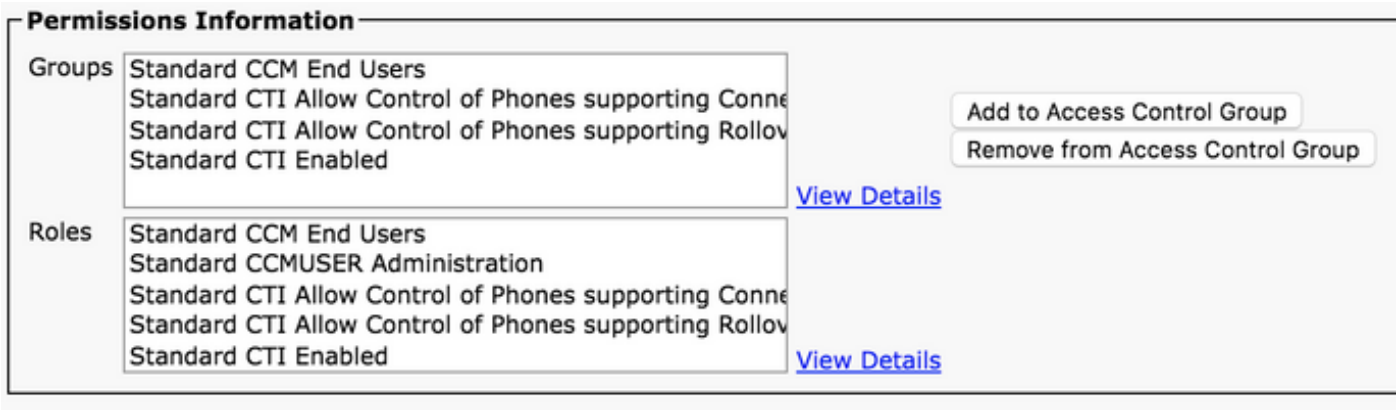
The table (Table 1.1) lists all the required roles, their privileges and the reason why Jabber needs the role assigned.

Table 1.1

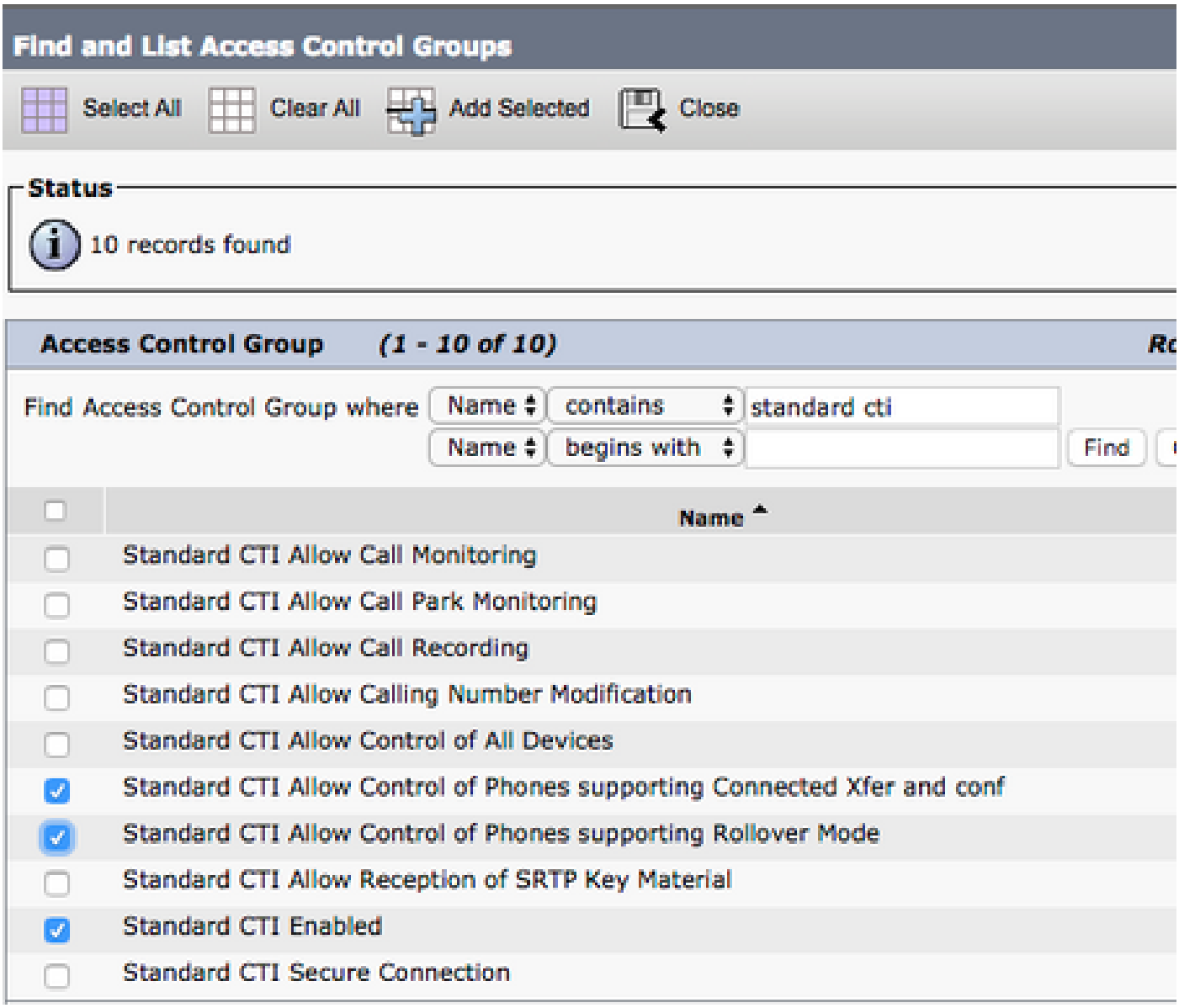
Roles	Privileges/Resources	Jabber Role Usage
Standard CCM End Users	Grant an end user log-in rights to the Cisco Unified CM User Options.	Jabber SOAP Authentication
Standard CCMUSER Administration	Allows access to the Cisco Unified CM User Options.	Jabber SOAP Authentication

Standard CTI Allow Control of Phones Supporting Rollover Mode	Allows control of all CTI devices that support rollover mode.	Used for CTI Control of Cisco Unified IP Phone 6900 series
Standard CTI Allow Control of Phones Supporting Connected Xfer and conf	Allows control of all CTI devices that support connected transfer and conferencing	Used for CTI Control of Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series
Standard CTI Enabled	Enables CTI application control.	Used for CTI control of all other Jabber compatible CTI devices.

To assign a permission group to the CUCM end user, select the **Add to Access Control Group** button.



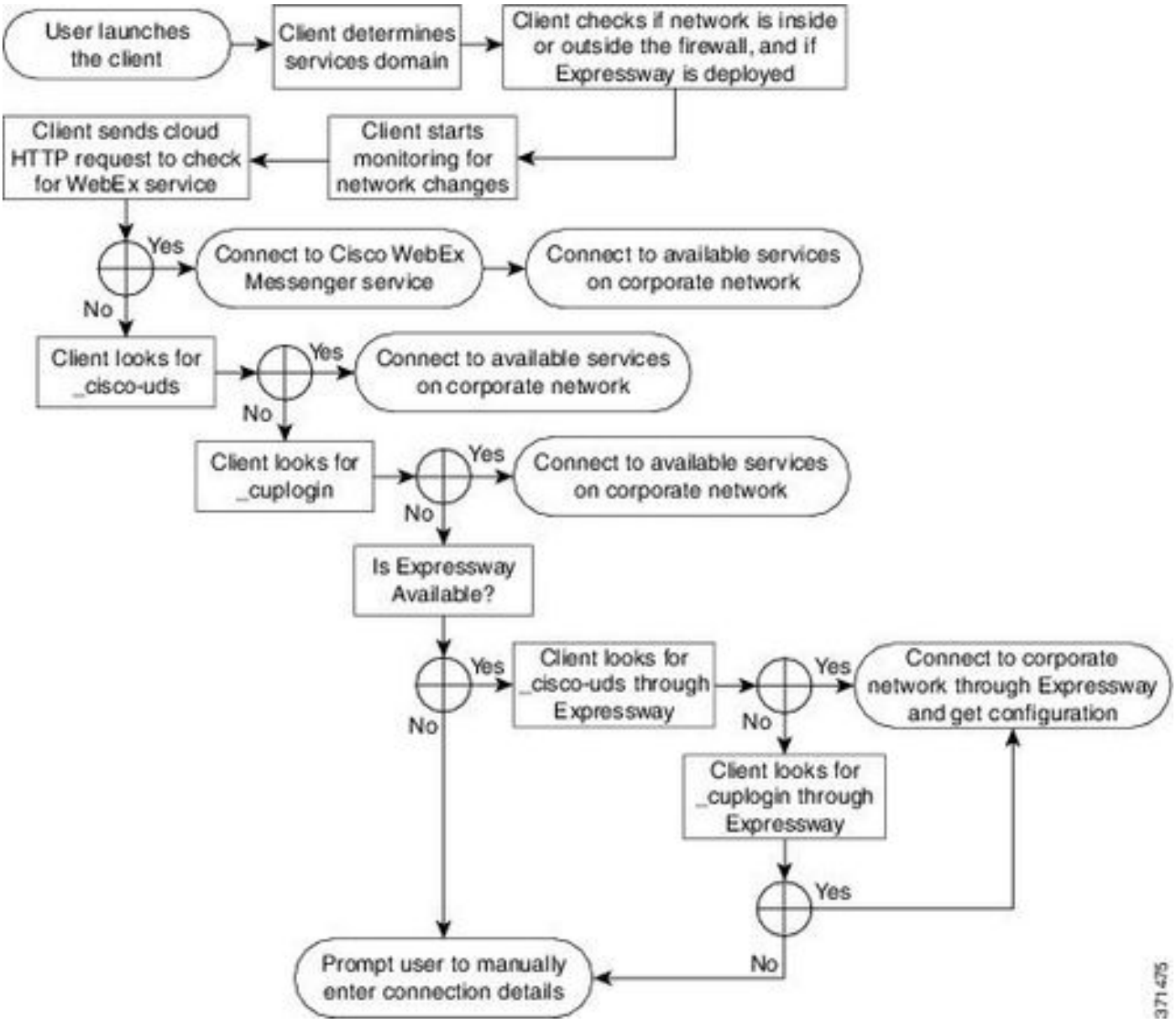
Then search for the access control group you would like to add and select the checkbox located near the access control groups name. When finished, select the **Add Selected** button.



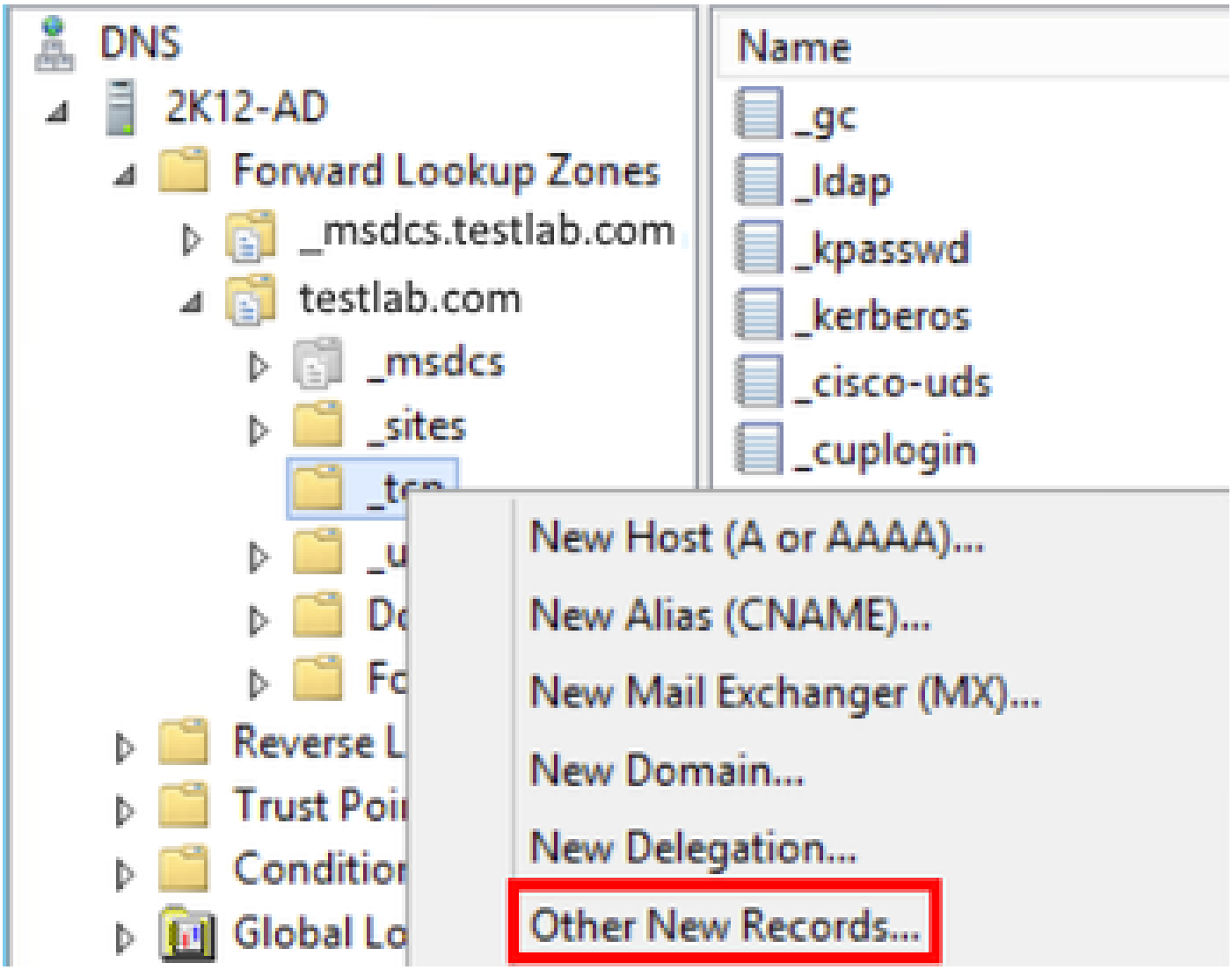
Service Discovery

For the Cisco Jabber client to be able to log in, it must first be aware of the services (CUCM, IM&P or Expressway) it uses for authentication and configuration retrieval. Cisco recommends set up automatic service discovery through the use of Domain Name System (DNS) Service Location (SRV) records as this provides a seamless user experience and ease of administration.

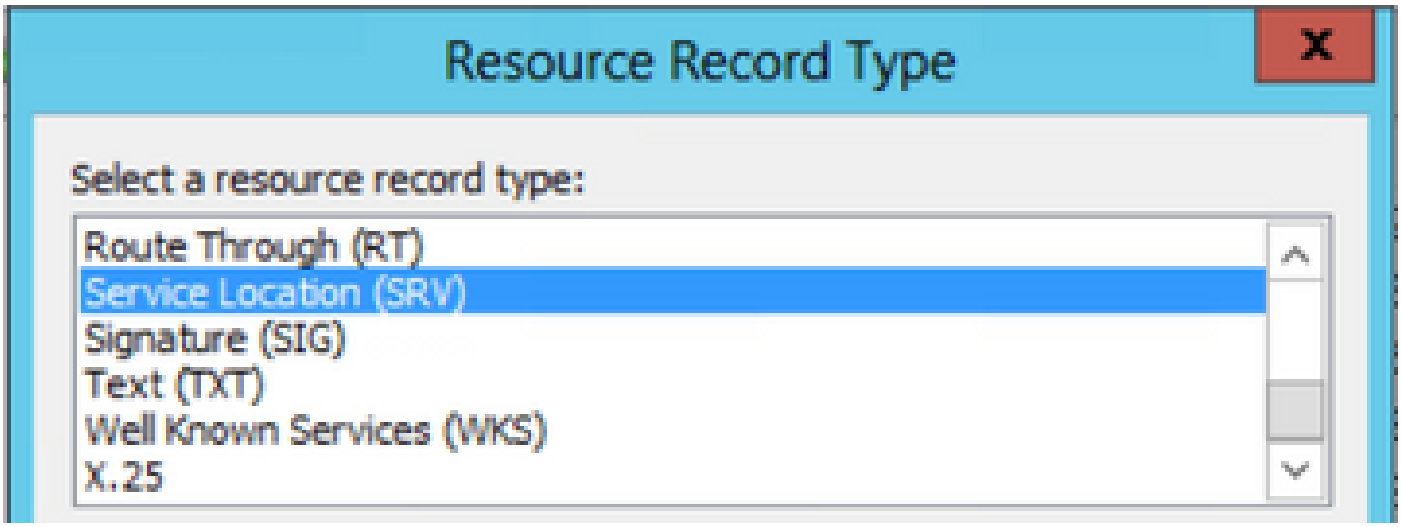
The image is graphical depiction of the Jabber automatic service discovery process.



To add DNS SRV record to Microsoft DNS Manager, navigate to your domain and expand the tree. Right click on the **_tcp** folder and select **Other New Records...**



When presented with the **Resource Record Type** window, highlight the **Service Location (SRV)** then select **Create Record...**



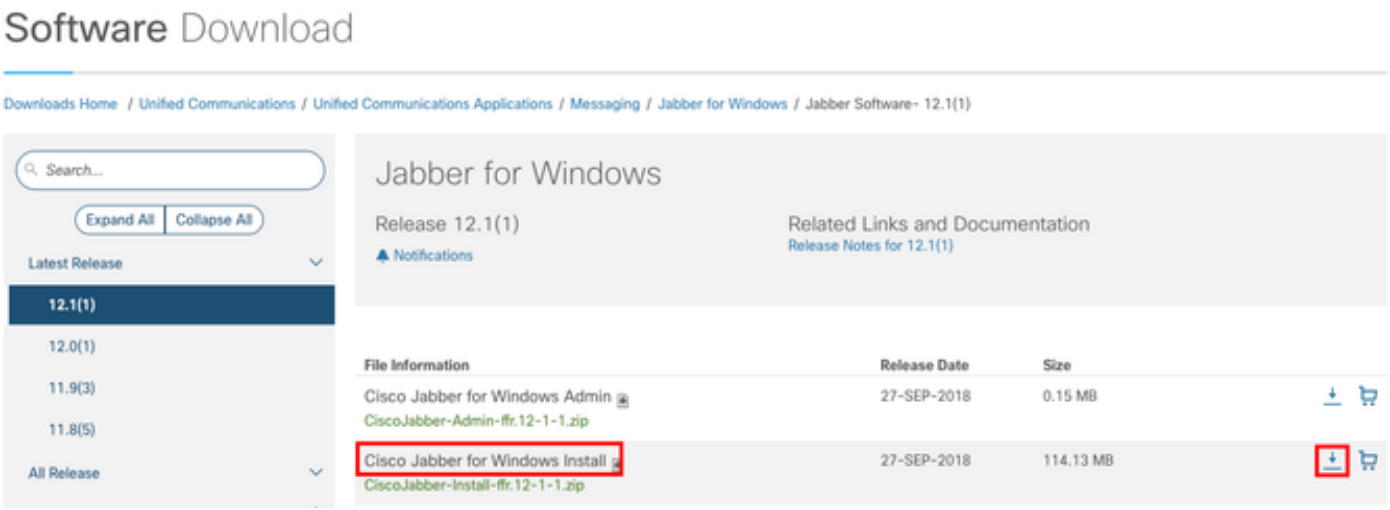
Next we see "New Resource Record" pane. Here, you can configure a SRV record for each of the CUCM servers that are to be used for Jabbers initial UDS home cluster lookup.

This is a configuration example for the_cisco-udsSRV record. In this example the _cisco-uds record resolves to three CUCM nodes within a CUCM cluster.

```
_cisco-uds._tcp.<domain_name>.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.<domain_name>.com
_cisco-uds._tcp.<domain_name>.com     SRV service location:
          priority       = 2
          weight         = 20
          port           = 8443
          svr hostname   = cucm2.<domain_name>.com
_cisco-uds._tcp.<domain_name>.com     SRV service location:
          priority       = 1
          weight         = 5
          port           = 8443
          svr hostname   = cucm1.<domain_name>.com
```

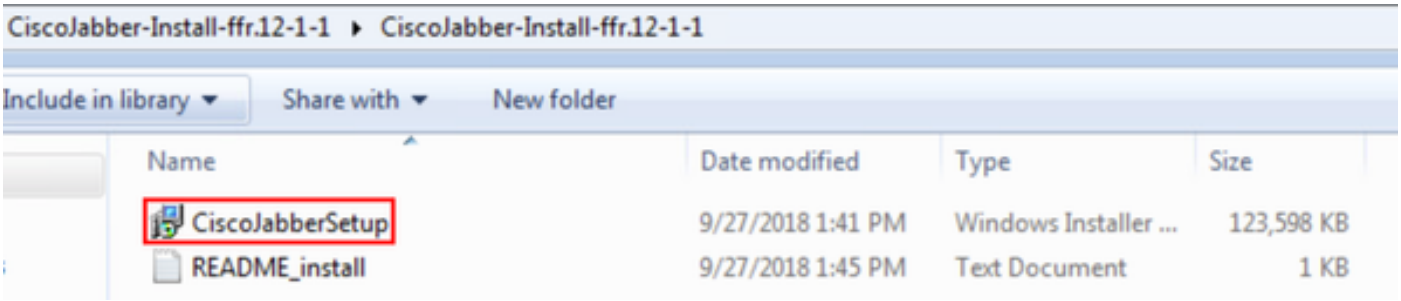
Download Jabber

Open your web browser of choice and navigate to https://software.cisco.com/download/home. Once on the download home page, search for Jabber for Windows. Once you are presented with download options, select the **Cisco Jabber for Windows Install** download as seen in the screenshot:



Installation of Jabber

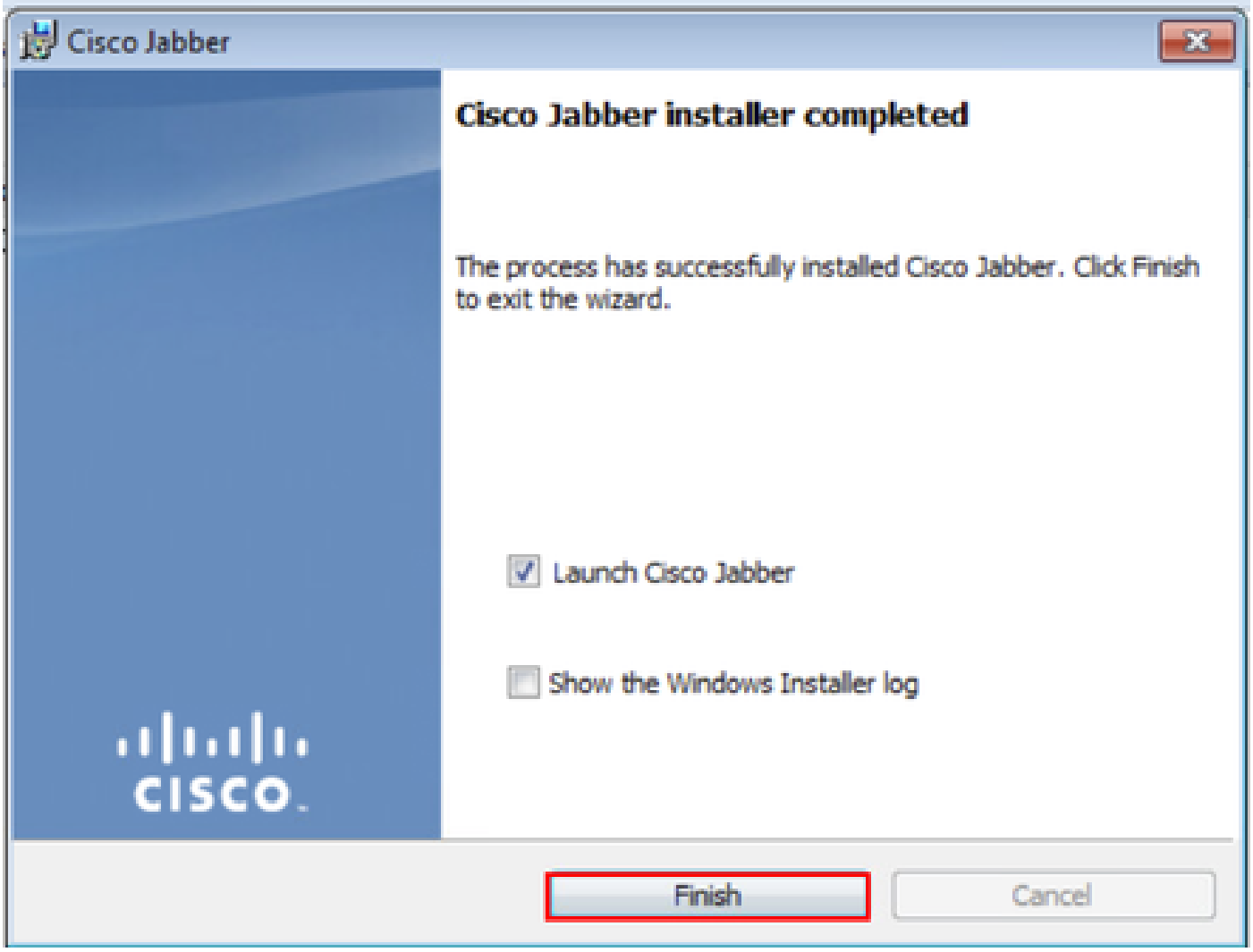
Choose the Cisco Jabber for Windows installer that you previously downloaded. Unzip the Jabber installation folder and select the **CiscoJabberSetup.msi.**



Once the Jabber for Windows installation launches, please read through the notices and disclaimers. If

you wish to continue with the installation, select **Accept and Install**.

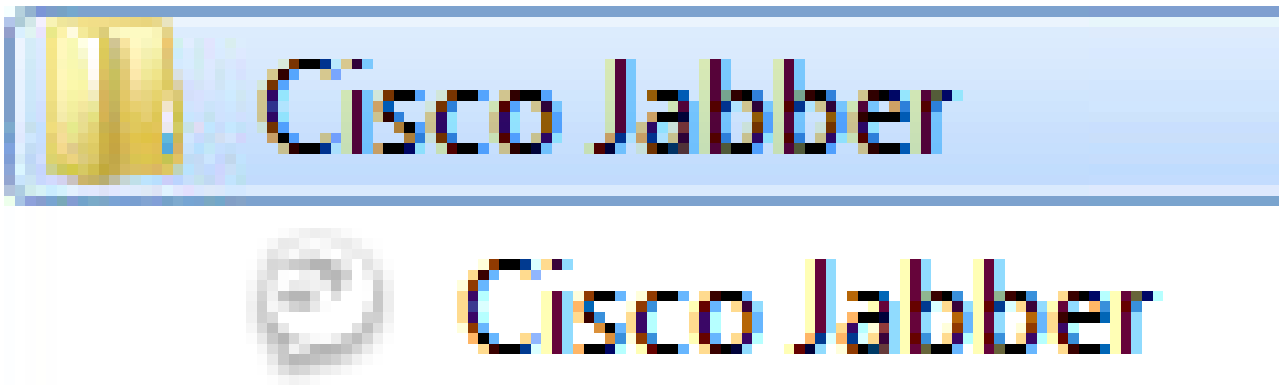
When the Jabber installation has finished, you are presented with the **Cisco Jabber installer completed** window. To complete the install, select **Finish**.



Log into Jabber

To perform a log in on Jabber for Windows, choose the Jabber application on the Microsoft Windows machine and launch it .

- Windows 7
  - Navigate to the **Windows Start Menu > All Programs > Cisco Jabber > Cisco Jabber** or select the Jabber desktop icon if applicable.

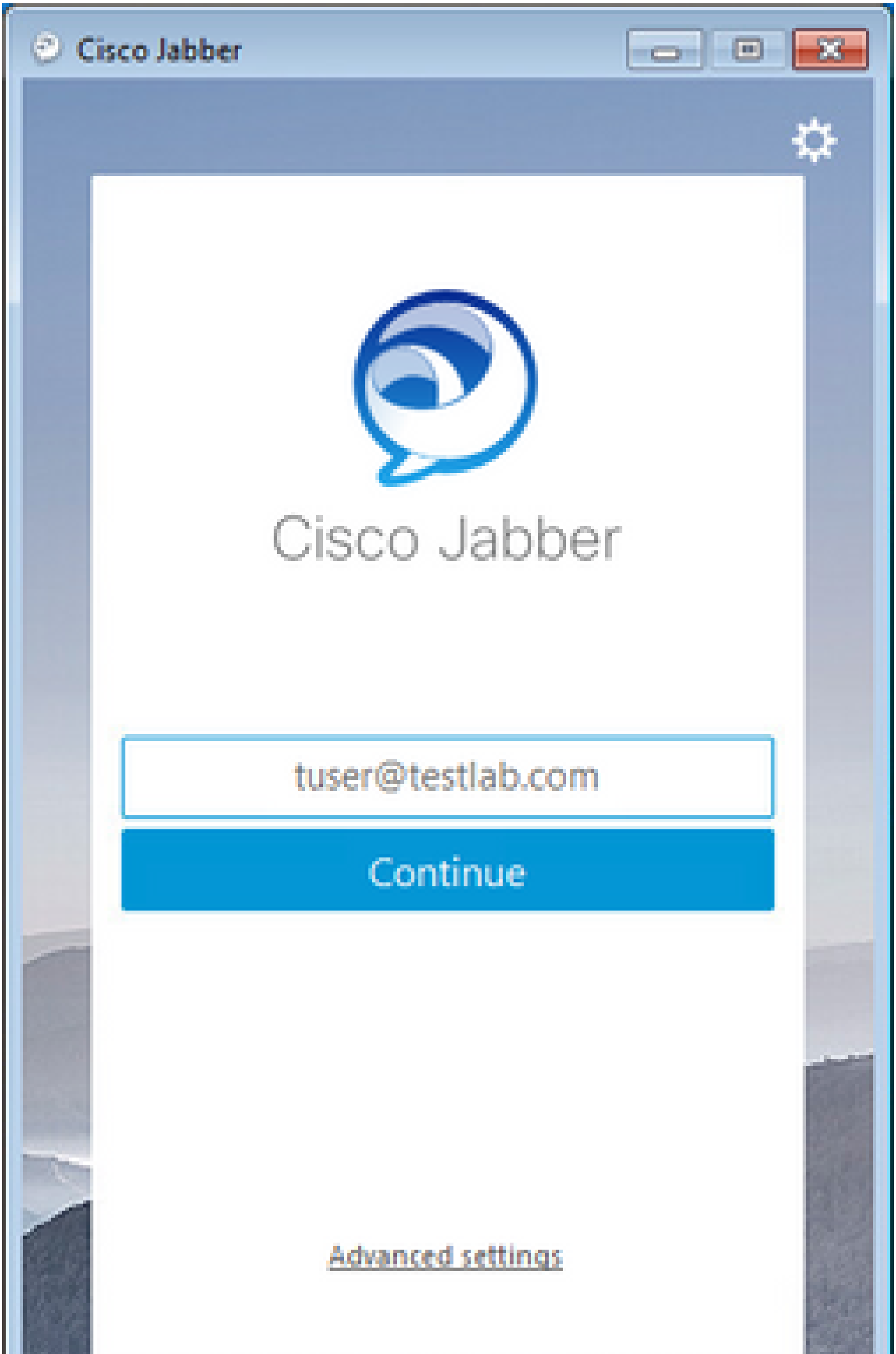


- Windows 10
  - Navigate to the **Windows Start Menu > Cisco Jabber > Cisco Jabber** or select the Jabber

desktop icon if applicable.

Once the Jabber application has been launched, provide the Jabber username and the domain that is used for service discovery (example. tuser@testlab.com).

Note: By default, Jabber uses the User Principal Name (UPN) of the logged in Windows session to retrieve the domain used for service discovery. The screenshot assumes that UPN discovery is not in use.


Cisco Jabber
Cisco Jabber
tuser@testlab.com
Continue
Advanced settings