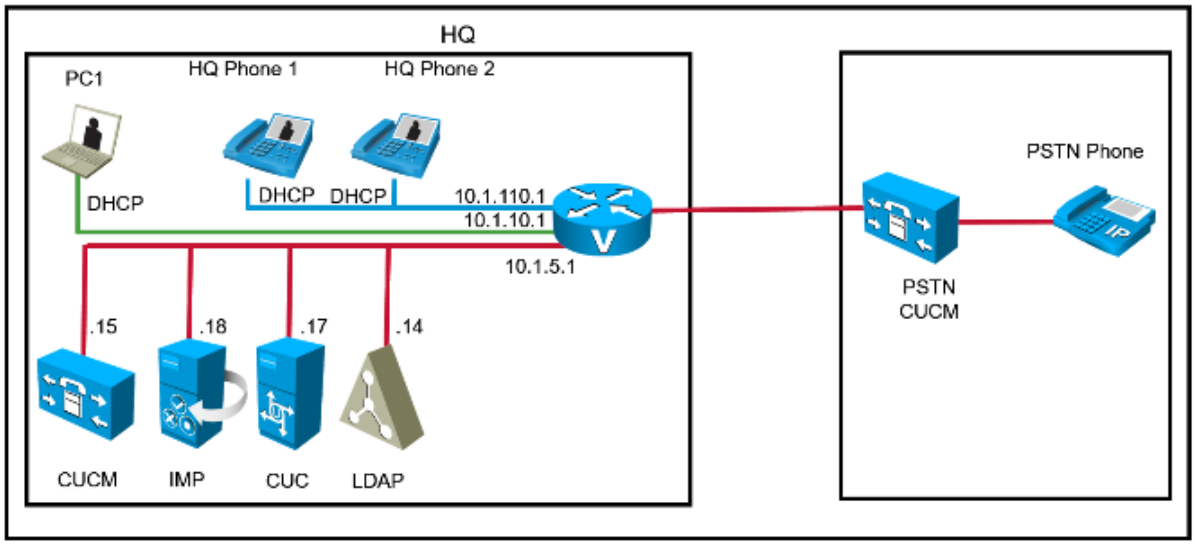
Implementing Cisco Collaboration Devices (CICD) v1.0

LAB GUIDE

- HQ Server Subnet 10.X.5.0/24
- HQ Data Subnet 10.X.10.0/24
- HQ Voice Subnet 10.X.110.0/24



Contents

LAB1: Explore Administrator Interfaces 5
Lab2: Explore End-User Interfaces 19
LAB3: Explore Call Flows in Cisco Unified Communications Manager 32
Job AIDS 32
LAB 4: Implement End Users 44
LAB5: Implement Endpoints 52
Lab6: Enable Telephony Features 64
LAB7: Enable Mobility Features 74
LAB8: Implement End Users and Voice Mailboxes 86
LAB9: Enable Cisco Unified Communications Manager IM and Presence Service 94
LAB10: Generate Cisco Unified Communications Manager CAR Tool Reports 107
LAB11: Monitor the System with Cisco Unified RTMT 109

LAB 1: Explore Administrator Interfaces

LAB1: Explore Administrator Interfaces

Start Services in Cisco Unified Communications Manager Serviceability

In this task, you will activate the necessary services on Cisco Unified Communications Manager for IP phone registration and reporting: Cisco CallManager, Cisco TFTP, and the Cisco Serviceability Reporter service.

Complete these steps:

Step 1

From the classroom PC, access Cisco Unified Communications Manager Serviceability pages with a web browser. Open the following URL: **https://10.1.5.15/ccmservice**.

Step 2

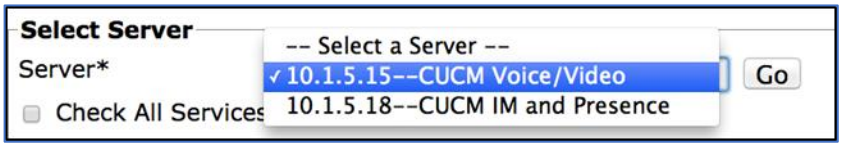
Log in with the username of **admin** and a password of **cicdpass1!**.

Step 3

Go to **Tools > Service Activation**.

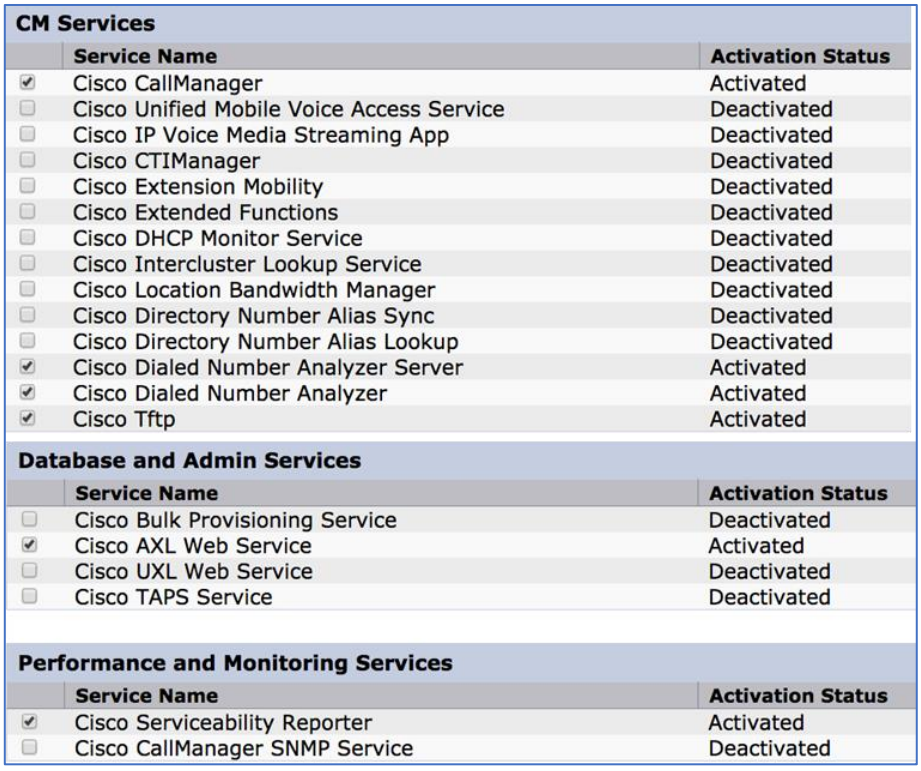
Step 4

From the Service Activation page, choose **10.1.5.15—CUCM Voice/Video** from the Select Server drop-down list and click **Go**.



Step 5

From the list of services, make sure that the Cisco CallManager, Cisco Tftp, Cisco Dialed Number Analyzer Server, Cisco Dialed Number Analyzer, Cisco Serviceability Reporter, and Cisco AXL Web Service services are activated. If they are not activated, check the check boxes for the services and click **Save** to activate these services. There will be a pop-up window that informs you that service activation will take a while. Click **OK** to confirm and wait for the page to refresh.



CM Services

	Service Name	Activation Status
☑	Cisco CallManager	Activated
☐	Cisco Unified Mobile Voice Access Service	Deactivated
☐	Cisco IP Voice Media Streaming App	Deactivated
☐	Cisco CTIManager	Deactivated
☐	Cisco Extension Mobility	Deactivated
☐	Cisco Extended Functions	Deactivated
☐	Cisco DHCP Monitor Service	Deactivated
☐	Cisco Intercluster Lookup Service	Deactivated
☐	Cisco Location Bandwidth Manager	Deactivated
☐	Cisco Directory Number Alias Sync	Deactivated
☐	Cisco Directory Number Alias Lookup	Deactivated
☑	Cisco Dialed Number Analyzer Server	Activated
☑	Cisco Dialed Number Analyzer	Activated
☑	Cisco Tftp	Activated

Database and Admin Services

	Service Name	Activation Status
☐	Cisco Bulk Provisioning Service	Deactivated
☑	Cisco AXL Web Service	Activated
☐	Cisco UXL Web Service	Deactivated
☐	Cisco TAPS Service	Deactivated

Performance and Monitoring Services

	Service Name	Activation Status
☑	Cisco Serviceability Reporter	Activated
☐	Cisco CallManager SNMP Service	Deactivated

Note: The Cisco CallManager service is responsible for call processing, while the Cisco Tftp service hosts the configuration files for the IP phones. The Cisco Serviceability Reporter service generates various daily reports, which can be accessed in the Cisco Unified Communications Manager Serviceability web interface.

Step 6

Browse to **Tools > Control Center – Feature Services**.

Step 7

At the Select Server page, choose **10.1.5.15—CUCM Voice/Video** and click **Go**.

Step 8

Verify that the Cisco CallManager, Cisco Tftp, and Cisco Serviceability Reporter services are started and activated.

Activity Verification

You have completed this task when you attain this result:

The services show the status Started and the activation status Activated.

Create a Personalized Application User and Verify Role Privileges for Application User Web Pages

In this task, you will create a personalized application user with your name and assign the rights to access the Cisco Unified Communications Manager Administration web interface. You will then enable dependency records in Cisco Unified Communications Manager enterprise parameters and verify the Application User Web Pages rights in the Standard CCMADMIN Administration role.

Complete these steps:

Step 9

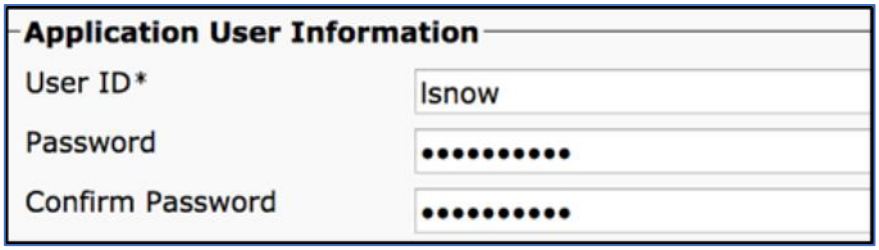
From the web browser, navigate to **https://10.1.5.15/ccmadmin** to open the Cisco Unified Communications Manager Administration web interface.

Step 10

Navigate to **User Management > Application User** and click **Add New**.

Step 11

Define a new application username with your user ID (for example, use “lsnow” for Linda Snow) and configure the password **cicdpass1!**.



Step 12

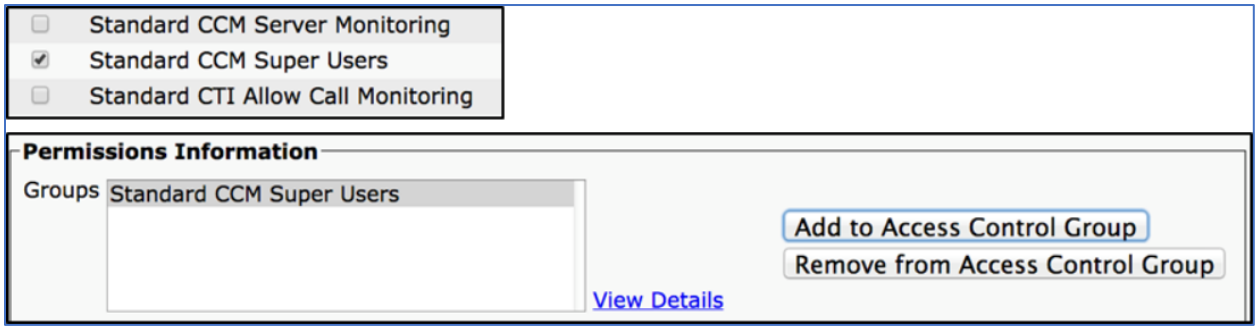
Scroll down and click **Add to Access Control Group**.

Step 13

In the pop-up window, click **Find** and search for the **Standard CCM Super Users** group.

Step 14

Check the box near the Standard CCM Super Users group and click **Add Selected** and then click **Save**.



Step 15

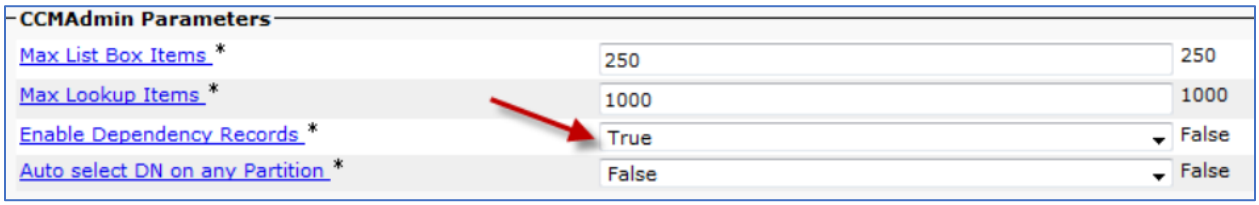
Log out with the administrator account and log in with the newly created application user and verify that the login is successful.

Step 16

In Cisco Unified Communications Manager, navigate to **System > Enterprise Parameters**.

Step 17

Set the Enable Dependency Records parameter to **True**. Click **OK** in the pop-up window. With dependency records, you can start a reverse search in Cisco Unified Communications Manager to determine, for example, which users belong to a certain device pool.



Step 18

Click **Save**.

Step 19

Click **Apply Config** and in the pop-up window click **OK**.

Step 20

Navigate to **User Management > User Setting > Access Control Group** and search the **Standard CCM Super Users** group. Click the hyperlink to open this group.

Step 21

Click **Find**. Your newly created user should appear in the list. Click the **I** icon to the right of your user. This lists all of the permissions for this user.

Step 22

Verify that for Application User Web Pages that both the read and update permissions are shown.

Step 23

Stay in the administration GUI for the next task.

Activity Verification

You have completed this task when you attain this result:

You can log in with the newly created application user and changes can be performed in Cisco Unified Communications Manager.

Add a New Cisco Unified IP Phone

In this task, you will create a new Cisco Unified IP video-capable phone with a directory number 2001 in the devices partition. You will select the preconfigured CSS of “pstn” for the device CSS. After you complete the configuration, you will verify the registration process.

Complete these steps:

Step 24

Start from the Cisco Unified Communications Manager Administration web interface.

Step 25

Navigate to **Device > Phone** and choose **Add New**.

Step 26

From the Phone Type drop-down list, choose **Cisco 7965** and then click **Next**. On the next screen, select SCCP as the device protocol, then click **Next**.

Step 27

Enter the MAC address of Phone Instance 1 of the Multilab Softphone (on the Phones PC). Since this is the first instance of the Multilab Softphone, use the MAC address of 111111111111 (the number 1, 12 times). On an actual Cisco Unified IP Phone, you would use the MAC address that is specified on the phone.

Step 28

In the Description field, enter **HQ Phone 1**.

Step 29

From the Device Pool drop-down list, choose **Default**.

Step 30

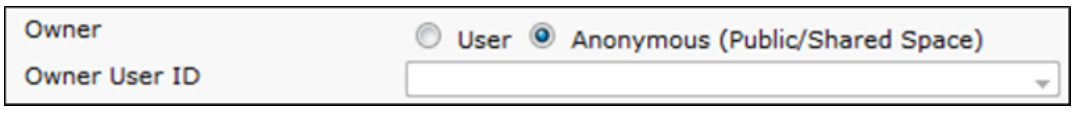
For the phone button template, choose **Standard 7965 SCCP**.

Step 31

Set the Calling Search Space value to **pstn**.

Step 32

To the right of the Owner field, click the **Anonymous (Public/Shared Space)** radio button.



Step 33

Set the Device Security Profile value to **Cisco 7965 – Standard SCCP Non-Secure Profile**.

Step 34

Click **Save** and apply the configuration.

Step 35

In the Phone configuration, click **Line [1] - Add a new DN** to create a new directory number.

Step 36

Enter **2001** in the Directory Number field. Press the **Tab** key to hop to the Route Partition field. The page refreshes to verify that the directory number exists.

Step 37

Choose **Devices** as the Route Partition value. Press the Tab key to hop to the next field.

After leaving the route partition field, Cisco Unified Communications Manager checks again for an existing directory number in the selected partition. Wait for the page to refresh.

Step 38

In the Alerting Name field, enter John Doe.

Step 39

Scroll approximately halfway down and enter **John Doe–2001** in the Line Text Label field and then click **Save**. If you get an error upon clicking **Save**, click **Save** again.

Step 40

Click **Apply Config** and **OK**.

Step 41

From the Phones PC, open the folder **Multilab** on the desktop. Open the **Setup Phones Wizard** application.

Step 42

In the TFTP Server field, enter **10.1.5.15**.

Step 43

In the MAC field, if there is already MAC addresses entered, delete them and enter **111111111111** (the dummy MAC address previously created in Cisco Unified Communications Manager).

Step 44

In the Phone Type drop down, select **7965**, then click **OK**.

Step 45

Double click the **Phone Instance 1** icon. The Phone instance should come up and you should see **2001** as the Directory Number and **Your Current Options** at the lower left of the phone display.

Step 46

In Cisco Unified Communications Manager, from the **Related Links**, choose **Configure Device (SEP<MAC>)** and click **Go**.

Step 47

Verify that the registration of the Cisco Unified IP Phone is successful and check the IP address of the registered device.

Step 48

Check the IP phone to verify that the display shows the configured directory number and line text label. The line text label will be shown on the upper right button.

Step 49

Repeat the previous steps in the Add a new Cisco Unified IP Phone section (Steps 41–48) to add HQ Phone 2 as instance 2 and PSTN Phone as instance 3, but make the MAC address **222222222222** (the number 2, 12 times) for HQ Phone 2 and **999999999999** (the number 9, 12 times) for the PSTN Phone. The PSTN phone will use the IP address of **10.140.1.15** as the TFTP Server (PSTN phone directory numbers are pre-configured).

Step 50

In the Phone configuration, click **Line [1] - Add a new DN** to create a new directory number.

Step 51

Enter **2002** in the Directory Number field. Press the **Tab** key to hop move to the Route Partition field. The page refreshes to verify that the directory number exists.

Step 52

Choose **Devices** for the Route Partition value.

After choosing the route partition, Cisco Unified Communications Manager checks again for an existing directory number in the selected partition. Wait for the page to refresh.

Step 53

In the Alerting Name field, enter **Jane White**.

Step 54

Scroll about halfway down the window and in the Line Text Label field, enter **Jane White–2002**. Click **Save**.

Step 55

Click **Apply Config** and click **OK**.

Step 56

On the Phones PC, Double click **Phone Instance 2**.

Step 57

Back on the Cisco Unified Communications Manager administration page, from the Related Links, choose **Configure Device (SEP<MAC>)** and click **Go**.

Step 58

Verify that the registration of the Cisco Unified IP Phone is successful and check the IP address of the registered device.

Step 59

Check the IP phone to verify that the display shows the configured directory number and line text label.

Step 60

Place a call from 2001 to 2002, answer the call. Verify that the call says “Connected”.

Activity Verification

You have completed this task when you attain these results:

The device configuration window on Cisco Unified Communications Manager shows the IP address and that it is registered with Cisco Unified Communications Manager.

A call is placed and answered between HQ Phone 1 and HQ Phone 2.

Modify Service Parameters

In this task, you will modify the service parameters on Cisco Unified Communications Manager to collect caller information for billing and reporting. The activation of the CDR and CMR service parameters is necessary for later labs. If you do not enable these parameters, Cisco Unified Communications Manager does not collect CDRs and CMRs.

Complete these steps:

Step 61

In the Cisco Unified Communications Manager Administration web pages, navigate to **System > Service Parameters**.

Step 62

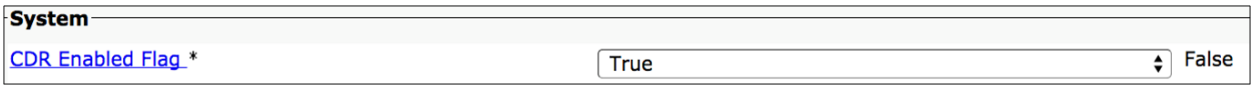
Choose the active server **10.1.5.15—CUCM Voice/Video** from the Active Server drop-down list.

Step 63

Choose the **Cisco CallManager** service.

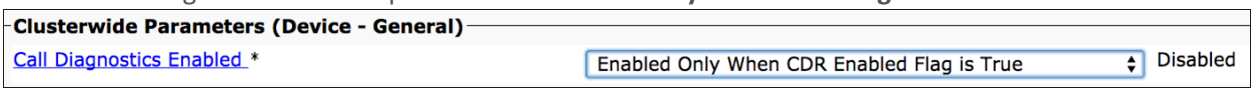
Step 64

Search for the CDR Enabled Flag field and set the parameter to **True**.



Step 65

Set the Call Diagnostics Enabled parameter to **Enable Only When CDR Flag is True**.



Step 66

Click **Save**.

Activity Verification

You have completed this task when you attain these results:

The CDR Enabled Flag is set to True and the Call Diagnostics Enabled parameter is set to Enabled Only When CDR Flag is True.

This task will be verified on the last day of training, where the calls of the week are viewed in Cisco Unified Communications Manager CDR Analysis and Reporting tool. The activation allows Cisco Unified Communications Manager to collect data over the week.

Verify the Application Server in Cisco Unified Communications Manager for Cisco Unified Communications Manager IM and Presence Service

In this task on the Cisco Unified Communications Manager, you will verify that the Cisco Unified Communications Manager IM and Presence Service is configured as an application server so that it will synchronize with the Cisco Unified Communications Manager.

Complete these steps:

Step 67

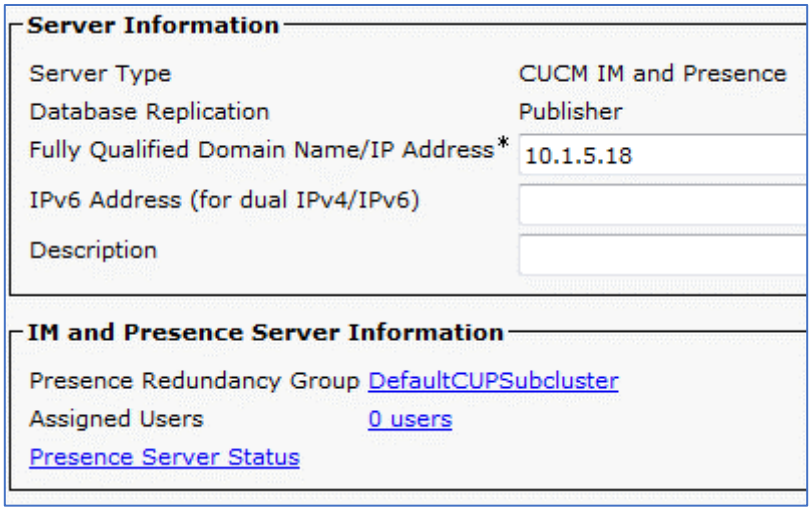
Use a browser to access the Cisco Unified Communications Manager Administration pages via the following URL: **https://10.1.5.15/ccmadmin**.

Step 68

Navigate to **System > Server** and choose the IM and Presence server that has the IP address of 10.1.5.18.

Step 69

View the preconfigured server settings and note that zero users are currently assigned to the IM and Presence server.



Activity Verification

You have completed this task when you attain this result:

The Cisco Unified Communications Manager IM and Presence Service server appears when you navigate to **System > Server**.

Enable Services on Cisco Unified Communications Manager IM and Presence

To support the Cisco Unified Personal Communicator registration process, in this task, you will activate the necessary services on Cisco Unified Communications Manager IM and Presence Service and verify that the services are running.

Complete these steps:

Step 70

Use a browser to access the Cisco Unified Presence Serviceability pages via the following URL: **https://10.1.5.18/ccmservice**.

Step 71

Navigate to **Tools > Service Activation**.

Step 72

From the Server drop-down menu, choose **10.1.5.18—CUCM IM and Presence**.

Step 73

Verify that the check boxes for the following services are checked, or check them if necessary:

Cisco AXL Web Service

Cisco SIP Proxy

Cisco Presence Engine

Cisco XCP Text Conference Manager

Cisco XCP Connection Manager

Cisco XCP Authentication Service

Step 74

Click **Save** and **OK** in the pop-up window.

Step 75

Navigate to **Tools > Control Center – Feature Services**.

Step 76

From the Server drop-down menu, choose **10.1.5.18—CUCM IM and Presence**.

Step 77

Verify that the activated services are running (started in contrast to starting).

Activity Verification

You have completed this task when you attain this result:

The previously listed services are active and running in the Feature Services configuration window.

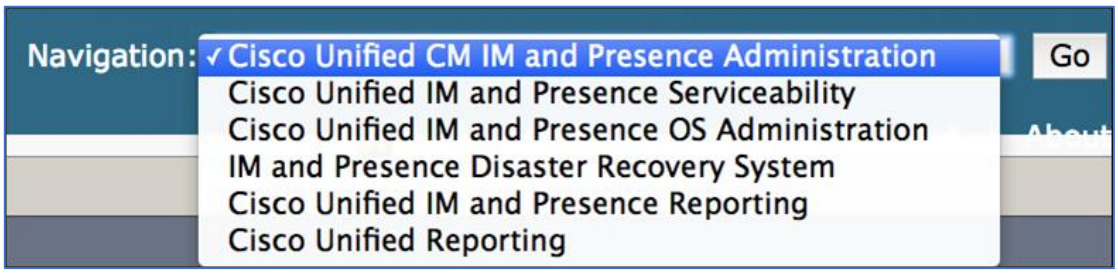
Create the Presence Gateway for Cisco Unified Communications Manager in the Cisco Unified Communications Manager IM and Presence Service

On Cisco Unified Communications Manager, the SIP trunk for presence subscription (for example, for on-hook or off-hook status) is already preconfigured. In this task, you will complete the configuration on the Cisco Unified Communications Manager IM and Presence Service server by adding a presence gateway. Use the IP address of the Cisco Unified Communications Manager as the gateway address.

Complete these steps:

Step 78

From your browser, choose **Cisco Unified CM IM and Presence Administration** from the navigation drop-down list and click **Go**.



Step 79

Navigate to **Presence > Gateways** and choose **Add New**.

Step 80

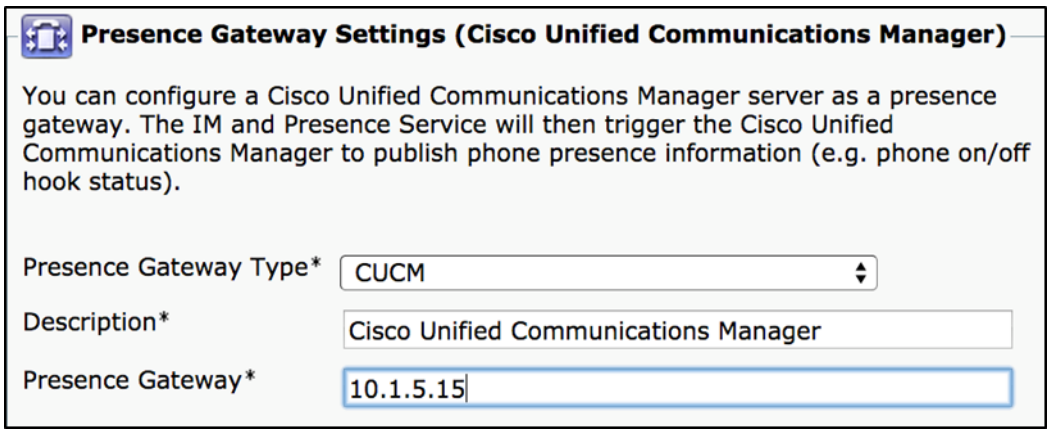
Choose **CUCM** as the presence gateway type.

Step 81

Enter **Cisco Unified Communications Manager** in the Description field.

Step 82

Enter **10.1.5.15** in the Presence Gateway field.



Step 83

Click **Save**.

Step 84

To verify, go back to the list of the gateways using Back to Find/List and click **Go**. Click **Find**.

Step 85

If the newly created gateway is listed, the gateway was created successfully.

Activity Verification

You have completed this task when you attain this result:

The Cisco Unified Communications Manager IM and Presence Service server displays Add Successful in the gateway find list.

Start the Cisco Serviceability Reporter Service

In this task, you will start the Cisco Serviceability Reporter service from the Cisco Unified Serviceability interface.

Complete these steps:

Step 86

Use the web browser to access the Cisco Unified Serviceability interface at **https://10.1.5.18/ccmservice**.

Step 87

Navigate to **Tools > Service Activation** and from the Server drop-down menu, choose **10.1.5.18—CUCM IM and Presence**.

Step 88

From the list of services, check **Cisco Serviceability Reporter** service.

Performance and Monitoring Services		
	Service Name	**Activation Status**
☑	Cisco Serviceability Reporter	Deactivated

Step 89

Click **Save** to activate the service. There will be a pop-up window that informs you that service activation will take a while. Confirm by clicking **OK**.

Step 90

Browse to **Tools > Control Center – Feature Services**.

Step 91

Verify that the Cisco Serviceability Reporter service is started and activated.

Activity Verification

You have completed this task when you attain these results:

The services show the status Started and the activation status Activated.

This task will be verified on the last day of training when the reports are generated. The activation allows Cisco Unity Connection to collect data over the week.

LAB 2: Explore End-User Interfaces

Lab2: Explore End-User Interfaces

Create an End User in Cisco Unified Communications Manager

In this task, you will create the end user, jdoe, in Cisco Unified Communications Manager and use jdoe as the user ID. You must also associate end users in Cisco Unified Communications Manager with a device. You will associate the previously configured IP phone with jdoe.

Complete these steps:

Create Users jwhite and jdoe

In this section, you will add a new user:

Step 1

From the classroom PC, access Cisco Unified Communications Manager Administration web pages with a web browser. Open the following URL: **http://10.1.5.15/ccmadmin**.

Step 2

Navigate to **User Management > End User** and click **Add New**.

Step 3

Create a user, Jane White, with the following settings and then click **Save**:

User ID: **jwhite**

Password: **cicdpass1!**

PIN: **131213**

Last Name: **White**

First Name: **Jane**

Step 4

Create a second user, John Doe, with the following settings and then click **Save**:

User ID: **jdoe**

Password: **cicdpass1!**

PIN: **131213**

Last Name: **Doe**

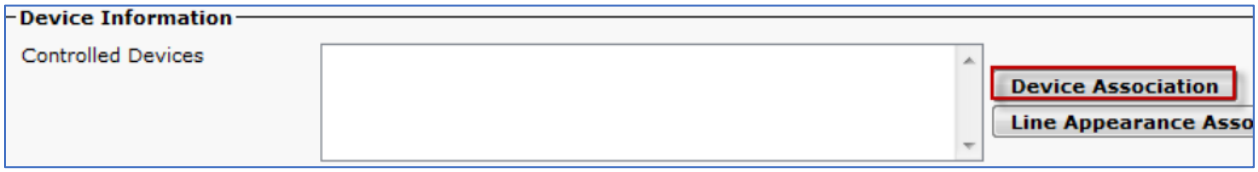
First Name: **John**

Associate the phone with the corresponding user

In this section, you will associate the previously created phones with jdoe and jwhite:

Step 5

On the End User page for jdoe, click **Device Association** on the End User Configuration page to associate the HQ Phone 1.



Step 6

In the new window that opens, search the IP phone by the previously defined description or directory number. Click **Find**.

Step 7

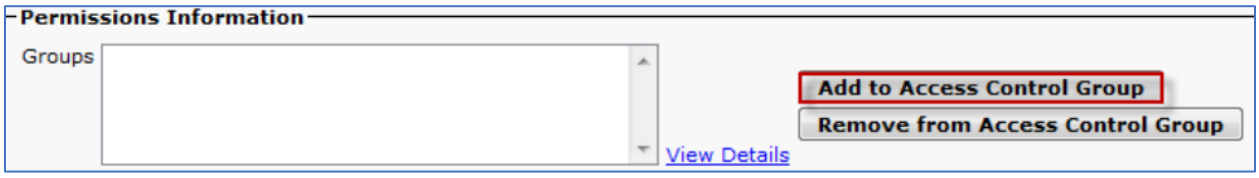
Check the check box near the HQ Phone 1 (2001) that you configured and click **Save Selected/Changes**.

Step 8

In the Related Links drop-down list, choose **Back to User** and click **Go**.

Step 9

Scroll down and click **Add to Access Control Group**.



Step 10

To allow end users to log into the web interface, choose the **Standard CCM End Users** and click **Add Selected**. Then, on the End User Configuration page, click **Save**.

Step 11

Repeat Steps 5–10 for the end user jwhite and HQ Phone 2.

Step 12

Log out of the Cisco Unified CM Administration website.

Note

When using the Cisco Unified CM Administration website and the Self Care Portal from the same browser, you cannot be logged into both simultaneously.

Test the jdoe User

In this section, you will test the jdoe login:

Step 13

Navigate to **http://10.1.5.15/ucmuser/** and use the newly created end user to log in.

Step 14

On the home page, you will see the available devices. Verify that the correct device name is displayed.

Step 15

On the left side, click **Phone Settings** or click the gear icon and then click **Settings**.

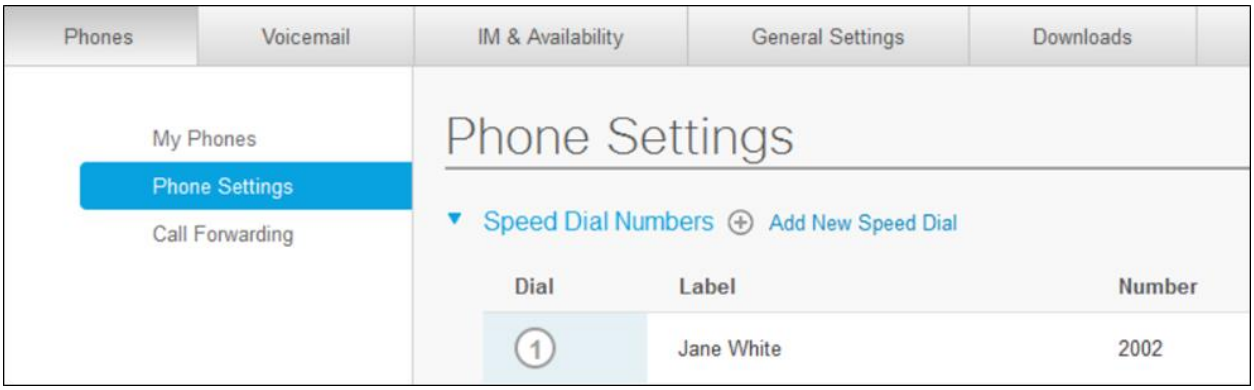
Step 16

Add a speed dial for Jane White with the following settings:

Number/URI: **2002**

Label (Description): **Jane White**

Speed Dial: **1**

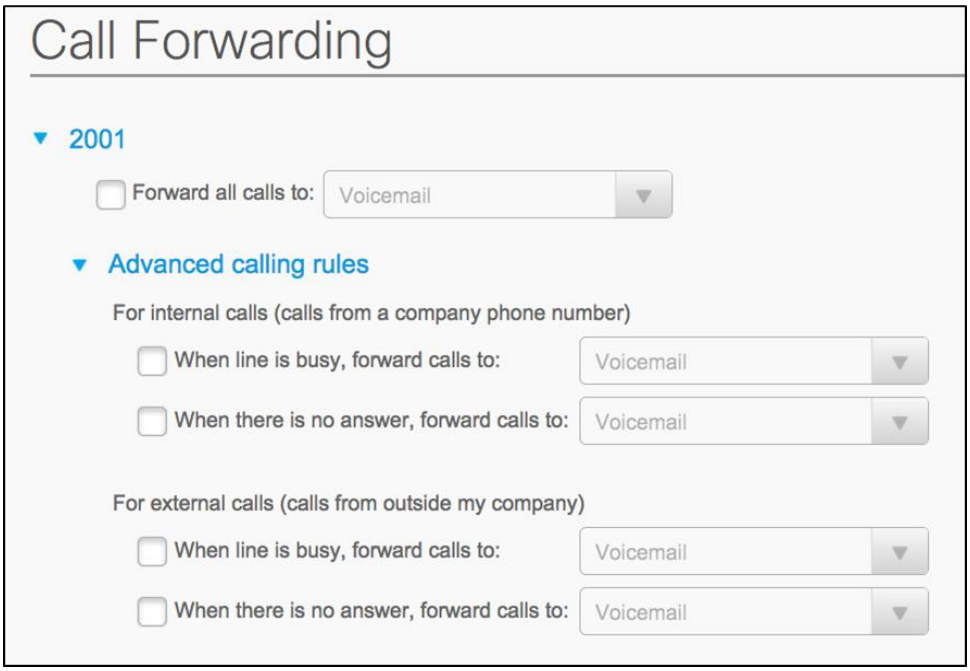


Step 17

In the Voicemail Notification Settings section, configure the settings to turn on the message waiting light and display a screen prompt when a new message is present and then click **Save**.

Step 18

On the left side, choose the **Call Forwarding** section and choose **Advanced Calling** rules. Notice that in addition to a general call forwarding setting, there are advanced calling rules that allow call forwarding to be configured for busy and no answer conditions, for both types: internal and external calls.



Step 19

To test the configured speed dial, from HQ Phone 1, press the third button from the top, labeled Jane White. 2002 should ring.

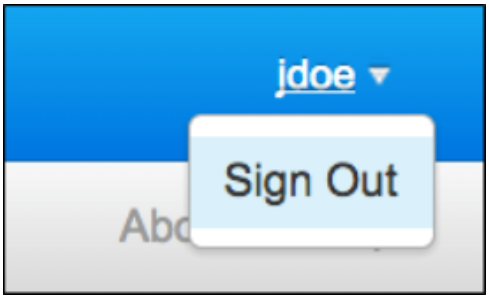
Step 20

To test the configured speed dial another way, press **1** (the index number of the speed dial), press the **AbbrDial** softkey button. The line on HQ Phone 2 should ring.

Note:The speed dial is on the third button because of the settings on the default 7965 phone button template. With this template, the first two buttons are set as lines and the rest of the buttons are set as speed dials. Because this is the speed dial that is assigned number 1, it is automatically associated to the top speed dial on the phone.

Step 21

In the upper-right corner of the web page, choose **jdoe** and then choose **Sign Out**.



Activity Verification

You have completed this task when you attain this result:

You successfully logged in to the end-user web interface and verified that the associated IP phone is associated to this user.

Set Enterprise Parameters and Configure End-User Settings

You can use the enterprise parameters to define which settings are visible in the end-user web interface. In this task, you will change the settings to display only the CFA option on the end-user interface and configure end-user settings. You will also set the CFA to voicemail with the end-user interface and configure the phone button below IP phone directory number as a speed-dial button to the directory number 2002.

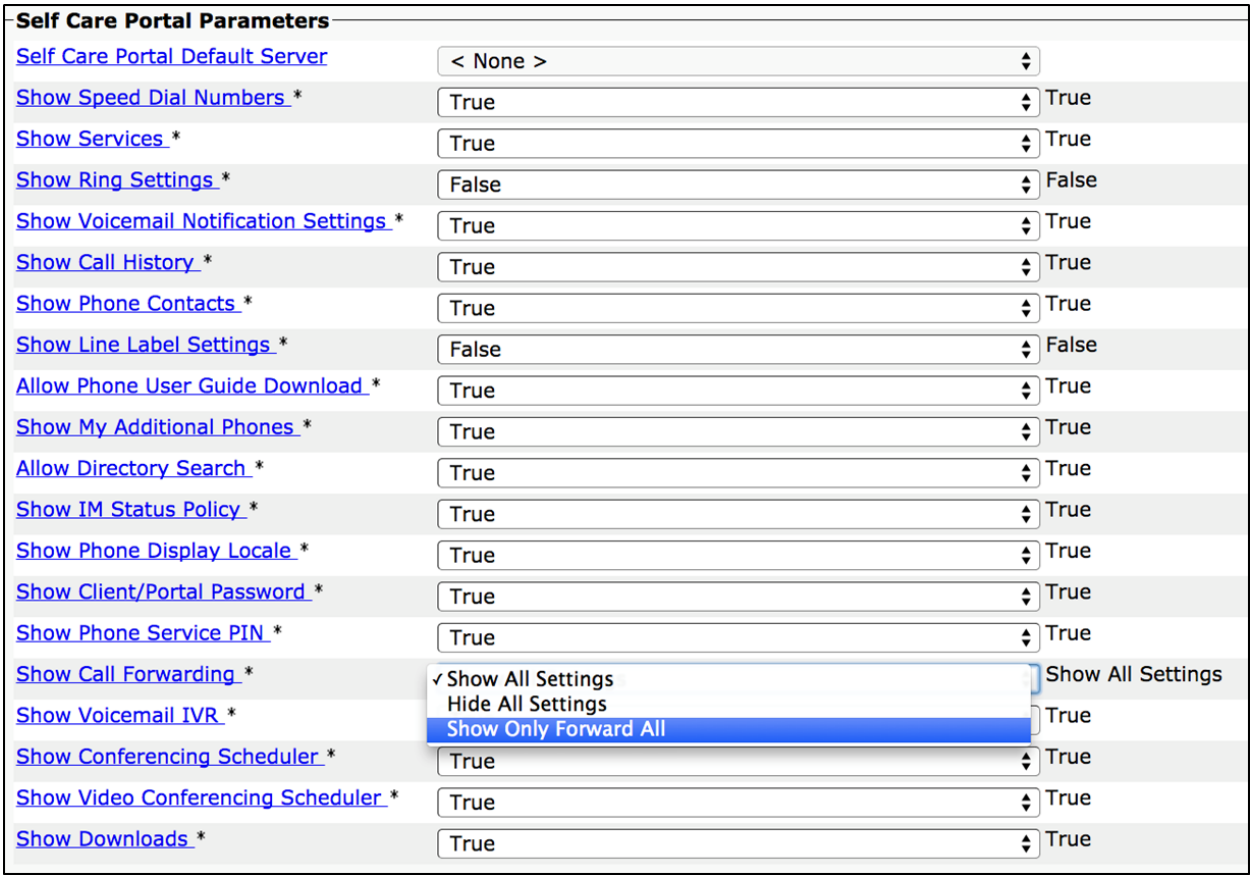
Complete these steps:

Step 22

In the Cisco Unified Communications Manager Administration web interface, navigate to **System > Enterprise Parameters**.

Step 23

In the Self Care Portal Parameters section, set the Show Call Forwarding parameter to **Show Only Forward All**.



Step 24

Click **OK** in the pop-up window.

Step 25

Click **Save** and click **Apply Config**.

Step 26

Click **OK**.

Step 27

Log out of the Cisco Unified Communications Manager administrative page. (This step is necessary, otherwise you may get an error logging into the Self Care Portal.)

Step 28

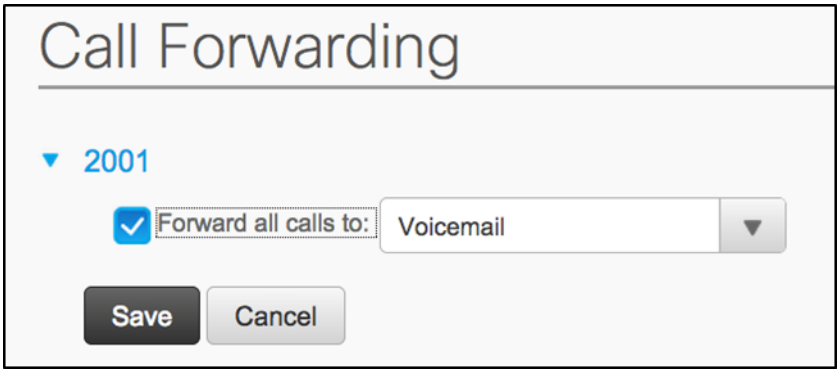
Navigate to **http://10.1.5.15/ucmuser/** and log in as jdoe.

Step 29

On the home page, choose **Call Forwarding**. Notice that the previously viewed advanced calling rules (for busy and no answer conditions, for internal and external calls) are no longer visible.

Step 30

To set the forwarding behavior to go to voicemail, check the **Forward All Calls** check box and choose **Voicemail** from the drop-down list.



Step 31

Click **Save**.

Step 32

On the IP phone display, verify that the phone displays “Forwarded to” and shows a flashing red arrow on the bottom right of the display screen.

Step 33

Log out of the Self Care Portal.

Step 34

Access Cisco Unified Communications Manager Administration web pages using a web browser. Open the following URL: **http://10.1.5.15/ccmadmin**.

Step 35

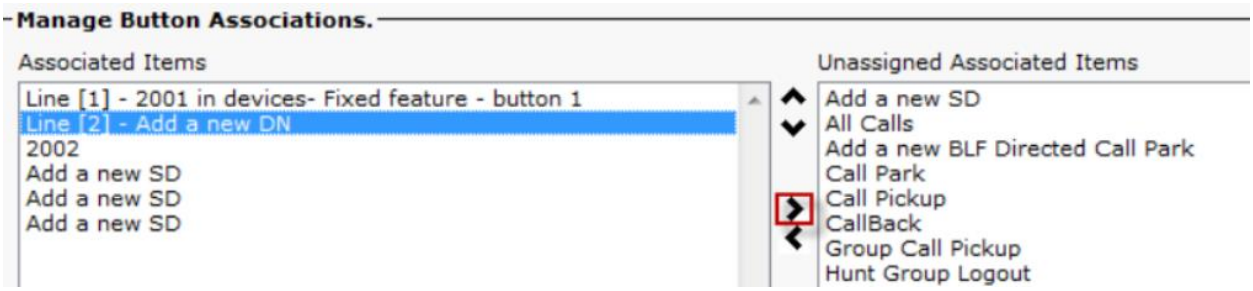
Navigate to **Device > Phone** and search for HQ Phone 1. Click the device name to enter the phone configuration.

Step 36

Click **Modify Button Items** and click **OK** in the pop-up window.

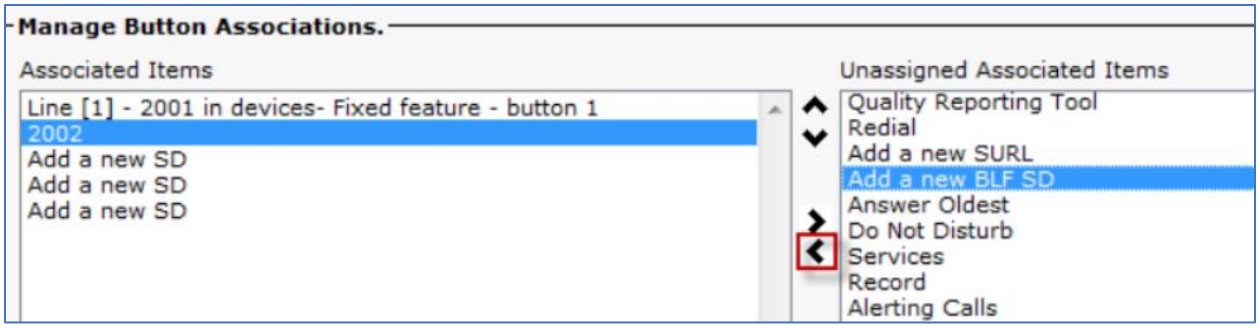
Step 37

Remove the second unused line from the Associated Items list with the arrow.



Step 38

Highlight **2002** and then, in the Unassigned Associate Items sections, choose **Add a new BLF SD**. If necessary, change the order of the buttons so that the speed dial to the directory number 2002 is displayed below the Line [1] - 2001 directory number and that the empty BLF speed dial is the third button.



Step 39

Click **Save** and **Close**. In the phone configuration window, save the changes and apply the configuration.

Step 40

Verify on the IP phone that the speed dial is now displayed on the second button below the directory number.

Step 41

From the HQ Phone 1, press the **CFwdAll** softkey to turn off the Forward All.

Activity Verification

You have completed this task when you attain these results:

The IP phone displays Forwarded to Voicemail

The configured speed dial is displayed below the directory number on the IP phone display.

Configure Voicemail Users in Cisco Unity Connection

To allow end users to use Cisco Unity Connection, in this task, you will create an end-user account and voice mailbox for jdoe. When the voice mailbox is configured, use the TUI to record a new name.

Complete these steps:

Step 42

Use the web browser to access Cisco Unity Connection administrator web interface at **https://10.1.5.17/cuadmin**.

Step 43

Choose **Users > Users** and click **Add New**. Enter the following information and then save:

Based on Template: **voicemailusertemplate**

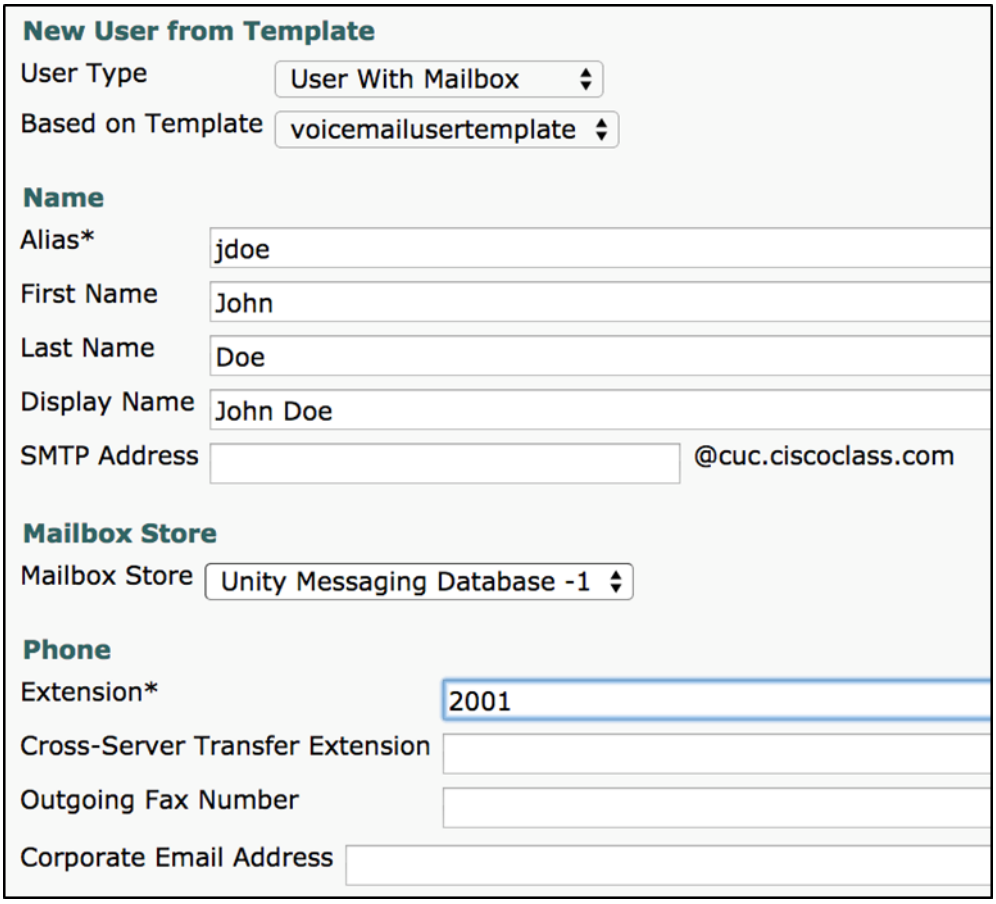
Alias: **jdoe**

First Name: **John**

Last Name: **Doe**

Display Name: **John Doe**

Extension: **2001**

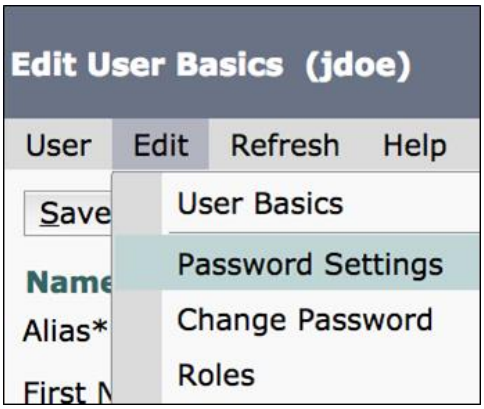


Step 44

Click **Save**.

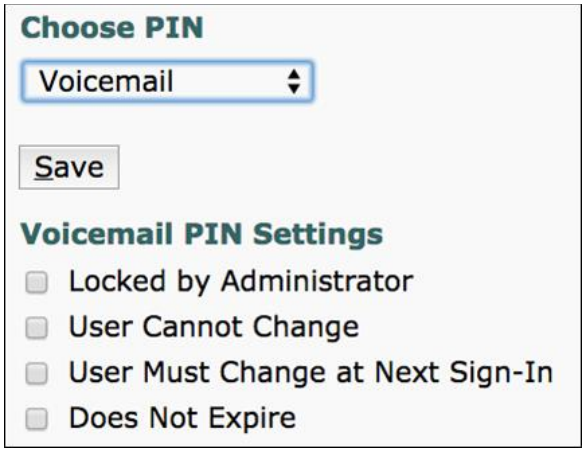
Step 45

Navigate to **Edit > Password Settings**.



Step 46

For the Voicemail, uncheck the **User Must Change at Next Sign-In** check box and then click **Save**.

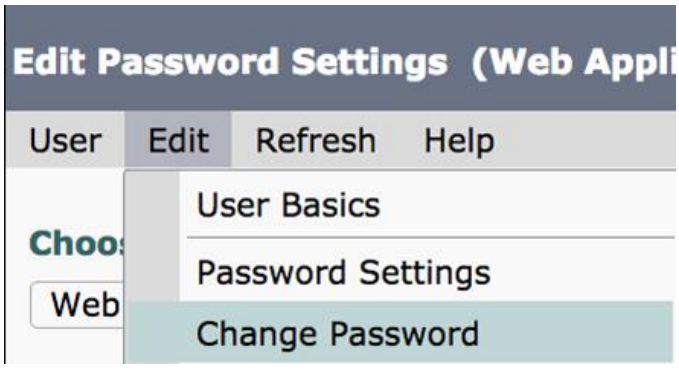


Step 47

For the Web Application, uncheck the **User Must Change at Next Sign-In** check box and then click **Save**.

Step 48

Navigate to **Edit > Change Password**.



Step 49

Set the voicemail PIN to **131213** and click **Save**.

Step 50

To verify that the voice mailbox is configured correctly, on the PC Desktop, click on the Cisco Unified Real-Time Monitoring Tool 10.5 icon.

Step 51

In the Host IP Address box, enter **10.1.5.17** and click OK. The username and password are the Cisco Unity Connection credentials. The application may take a few seconds to become operational.

Step 52

Select **Default** in the Configuration List box and click **OK**.

Step 53

In the top of the toolbar, select **Cisco Unity Connection** and select **Port Monitor**.

Step 54

In the Node box, select **cuc.ciscoclass.com**.

Step 55

At the bottom of the page, click **Start Polling**.

Step 56

Press the **Messages** button on the IP phone of user jdoe. Cisco Unity Connection answers and requires entering the user PIN. Notice the display on the IP Phone will say 2500.

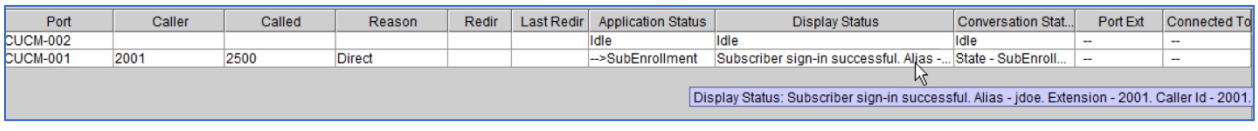
This is the pilot number of the Cisco Unity Connection system.

Watch the Port Monitor display and you will notice the calling number (2001), the called number(2500), and the voicemail port that answered the call.

Port	Caller	Called	Reason	Redir	Last Redir	Application St..	Display Status	Conversation...
CUCM-002						Idle	Idle	Idle
CUCM-001	2001	2500	Direct			-->SubAuthe...	Subscriber S...	State - SubA...

Step 57

Enter the user PIN and confirm with the pound sign (#) on the IP Phone. In Port Monitor, notice that the Display Status now indicates that the sign-in was successful. Hover over to see all relative information.



Step 58

Repeat Steps 2–13 for jwhite with extension 2002.

Activity Verification

You have completed this task when you attain this result:

The end-user voice mailbox can be accessed with the Messages button and the user can successfully sign in with the assigned PIN.

LAB 3: Explore Call Flows in Cisco Unified Communications Manager

LAB3: Explore Call Flows in Cisco Unified Communications Manager

Complete this lab activity to practice what you learned in the related module.

Upon completing this guided lab, you will be able to:

Configure a Cisco Unified Communications Manager CoS implementation

Configure the Cisco Unified Communications Manager call routing implementation

Test the inbound Cisco Unified Communications Manager CoS implementation

Configure the partition on the route patterns

Job AIDS

These job aids are available to help you complete the lab activity.

IP Addresses	
Device	IP Address
Cisco Unified Communications Manager	10.1.5.15
Cisco Unity Connection	10.1.5.17
Cisco Unified Communications Manager IM and Presence Service	10.1.5.18

Usernames and Passwords	
Device	Credentials
Cisco Unified Communications Manager Application User	User: admin Password: cicdpass1!
Cisco Unified Communications Manager Platform User	User: admin Password: cicdpass1!
Cisco Unity Connection Application User	User: admin Password: cicdpass1!
Cisco Unity Connection Platform User	User: admin Password: cicdpass1!
Cisco Unified Communications Manager IM and Presence Service Application User	User: admin Password: cicdpass1!
Cisco Unified Communications Manager IM and Presence Service Platform User	User: admin Password: cicdpass1!

Configure the Cisco Unified Communications Manager CoS Implementation

In this task, you will configure the Cisco Unified Communications Manager CoS implementation.

Complete these steps:

Step 1

From the classroom PC, access Cisco Unified Communications Manager Administration pages using the URL **http://10.1.5.15/ccmadmin**.

Step 2

Navigate to **Call Routing > Class of Control > Partition**.

Step 3

Click **Add New** and enter the name **P_Local**, followed by **P_National** in the next line, followed by P_International, and P_Block_National. Click **Save**.

Note:Even if multiple CSSs use the same partitions, you must create a partition only once.

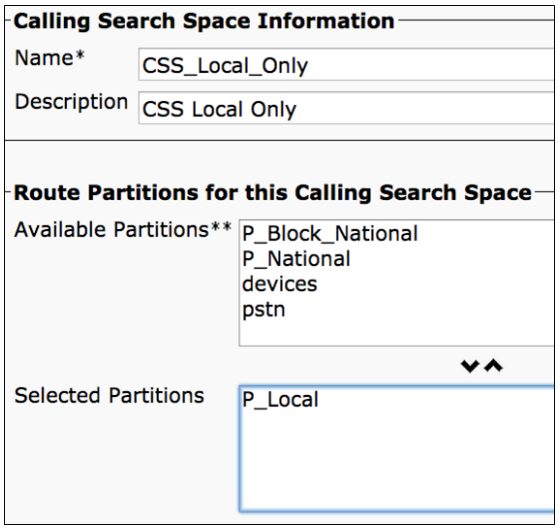
Step 4

Add the following CSSs and their associated partitions, according to the table. Each CSS will contain at least one partition. See the following steps for details.

CSS	Partitions
CSS_Local_Only	P_Local
CSS_National_Only	P_National
CSS_Block_National	P_Local, P_Block_National
CSS_Local_National	P_Local, P_National
CSS_Local_National_Intl.	P_Local, P_National, P_International

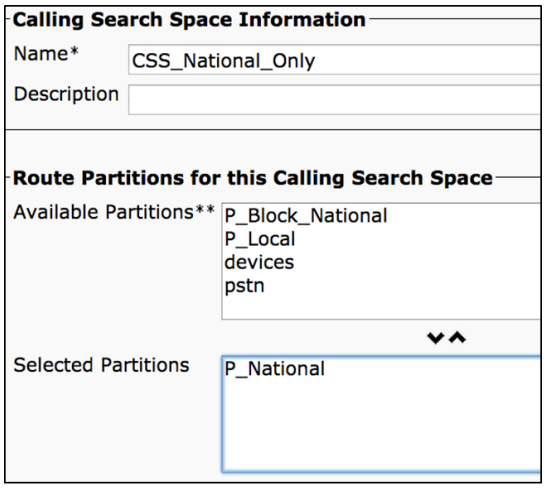
Step 5

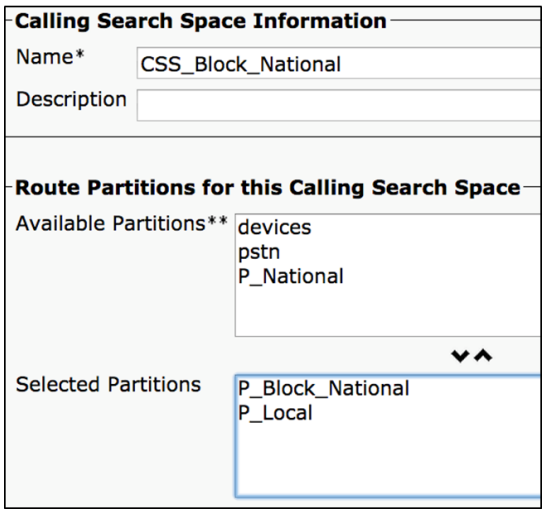
Navigate to **Call Routing > Class of Control > Calling Search Space** and click **Add New**. Enter the name **CSS_Local_only**. Choose the partition **P_Local** and move it to the Selected Partitions window, and click **Save** to save the configuration.



Step 6

Repeat Step 6 for the **CSS_National_only**, **CSS_Block_National**, **CSS_Local_National**, and **CSS_Local_National_Intl**.





Activity Verification

You have completed this task when you attain this result:

You have configured partitions and CSSs within CoS on Cisco Unified Communications Manager.

Configure the Cisco Unified Communications Manager Call Routing Implementation

In this task, you will configure the Cisco Unified Communications Manager call routing implementation.

Complete these steps:

Create SIP Trunk to PSTN

In this section, you will create the SIP trunk to the PSTN in Cisco Unified Communications Manager.

Step 7

In the Cisco Unified Communications Manager Admin page, click on **Device>Trunk**. There will be several predefined trunks visible.

Step 8

Click on **Add New**. In the Trunk Type box, select **SIP Trunk** and click **Next**.

Step 9

In the Device Name box, type **PSTN_Trunk**. Select the **Default Device Pool**, then scroll down to the SIP information section.

Step 10

In the Destination Address box, type **10.140.1.15**. In the SIP Trunk Security Profile, select **Non Secure SIP Trunk Profile** and in the SIP Profile box, select **Standard SIP Profile**.

Step 11

Click **Save**, then reset the newly created SIP Trunk.

Create Route Patterns

In this section, you will create route patterns in Cisco Unified Communications Manager.

Before completing these steps, click on the pre-configured route patterns that use **10.1.5.1** as the associated device and change the Gateway/Route List to **PSTN_Trunk**, and click save.

Step 12

Create new route patterns using the Copy feature. Assign the newly created partitions to the new route patterns. Navigate to **Call Routing > Route/Hunt > Route Pattern** and click **Find**.

Note:Using a different partition for each (destination) route allows for different classes of service to be implemented.

Step 13

Click the **Copy** icon on the right side of the 112 route pattern.

Step 14

Enter the following and save the configuration:

Route Pattern: **0.[1-9]XXXXXX**

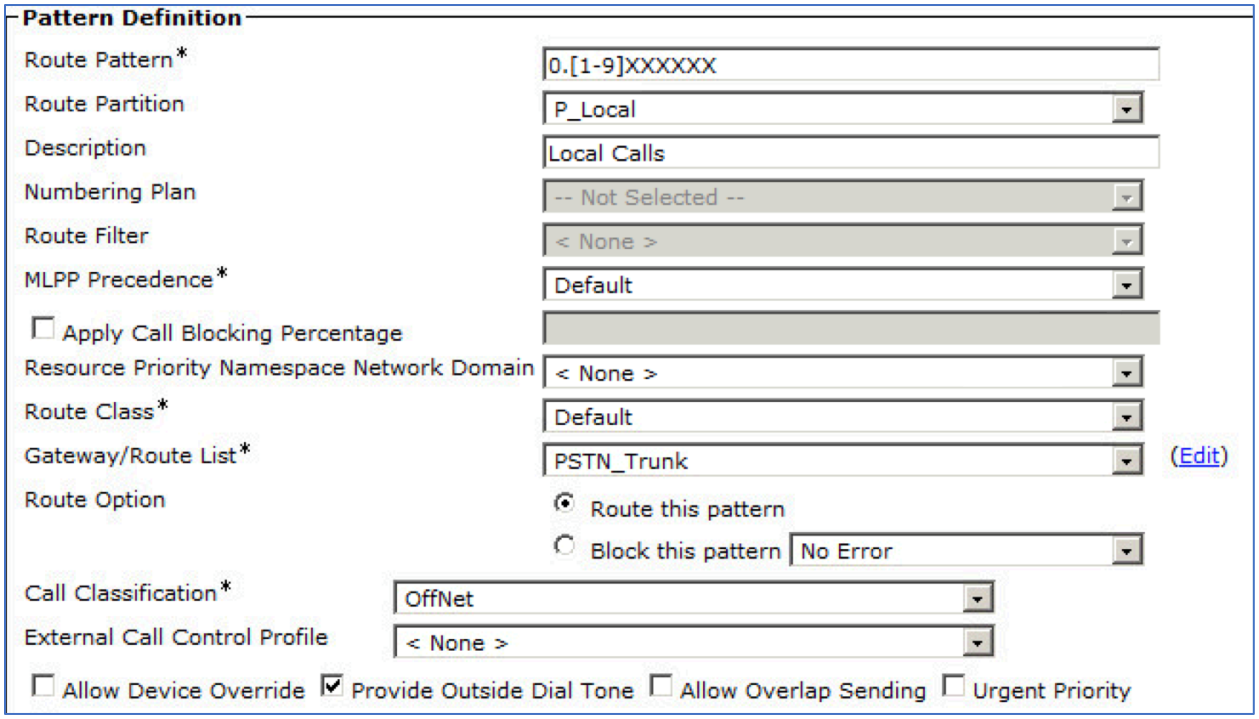
Route Partition: **P_Local**

Description: **Local calls**

Gateway/Route List: **PSTN_Trunk**

Check this box: **Route this Pattern**

Uncheck this box: **Urgent Priority**



Step 15

Click **Save** and then click **OK** in the two pop-up windows that appear.

Step 16

To create another new route pattern, click **Copy**.

Step 17

Enter the following and save the configuration:

Route Pattern: **0.0[1-9]XXXXXXXXX**

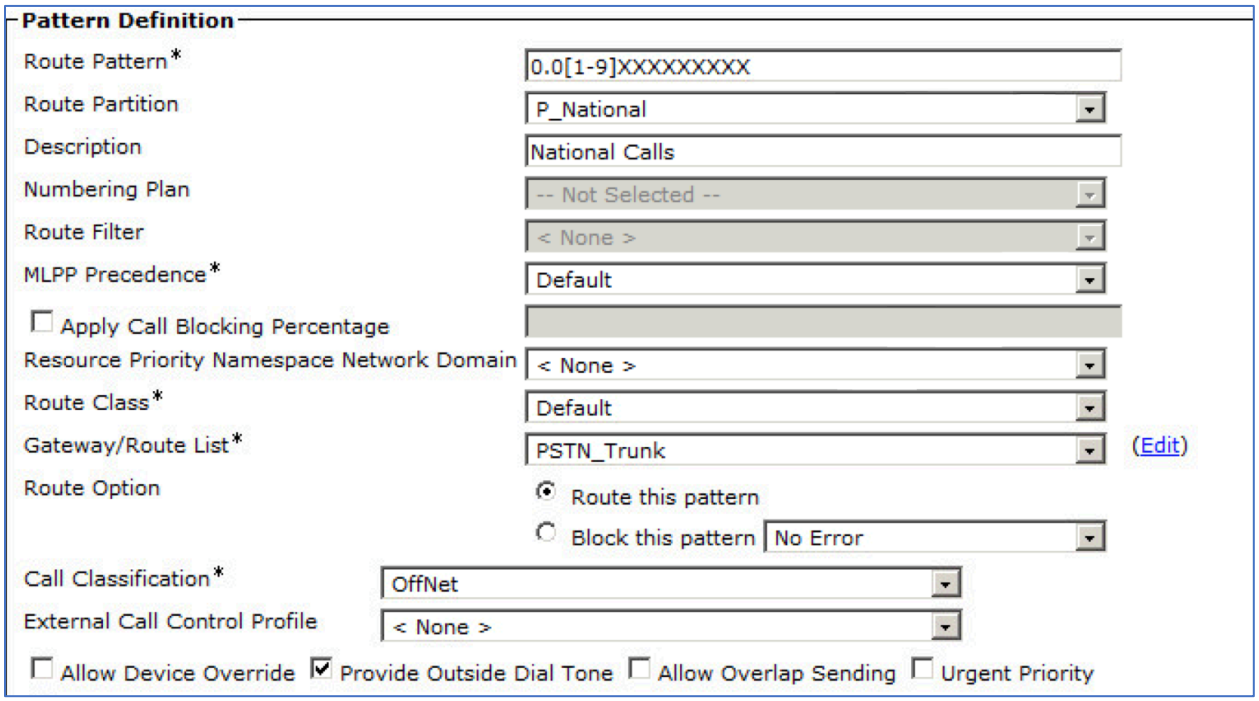
Route Partition: **P_National**

Description: **National calls**

Gateway/Route List: **PSTN_Trunk**

Check this box: **Route this pattern**

Uncheck this check box: **Urgent Priority**



Step 18

Click the **Save** button and then click **OK** in the two pop-up windows that appear.

Step 19

To create another new route pattern, click the **Copy** button.

Step 20

Enter the following and save the configuration:

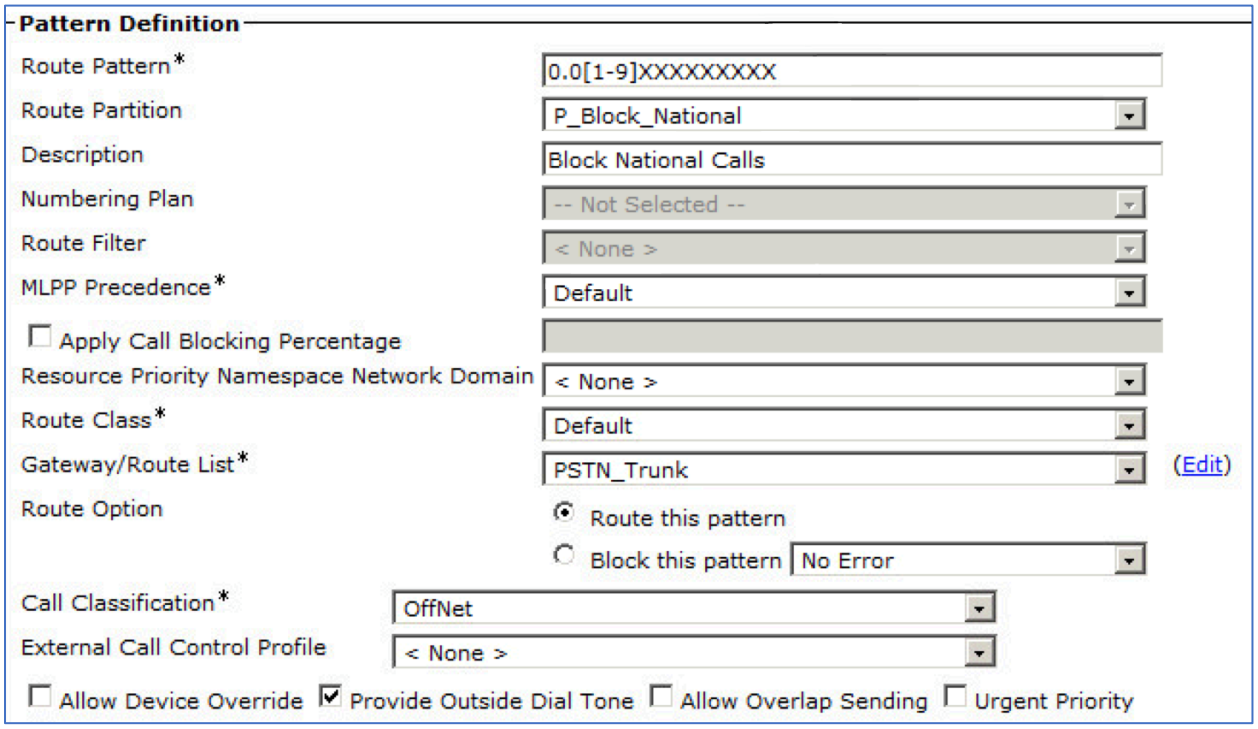
Route Pattern: **0.0[1-9]XXXXXXXXX**

Route Partition: **P_Block_National**

Gateway/Route List: **PSTN_Trunk**

Description: **Block national calls**

Check this check box: **Block this pattern**



Step 21

Click **Save** and then click **OK** in the two pop-up windows that appear.

Step 22

In the Related Links drop-down list, which is prepopulated with Back to Find/List, click **Go**.

Step 23

Choose the **000.[1-9]XXXXXXXXXXX** route pattern and change the partition to **P_International**.

Test Route Patterns for HQ Phone 2

In this section, you will test the route patterns that you added.

Step 24

Test the new route patterns one at a time by changing the CoS for HQ Phone 2. For testing, only one partition will be accessible at a time. Navigate to **Device > Phone** and click **Find**. Choose **HQ Phone 2**.

Step 25

Verify the following device parameter and save:

Calling Search Space: **pstn**

Step 26

Choose the first line on the device (2002). Change the following line parameter, then save and apply the configuration:

Calling Search Space: **CSS_Local_only**

Note:The line and device CSSs are joined to provide the CoS when calling from extension 2002. Testing is less complex if you use a single CSS on either the line or the device. In most live implementations, there may be both line and device CSSs.

Each time that you change the Calling Search Space, you must save the and apply the configuration (or reset the phone) for the new calling search space to be applied.

Step 27

Predict which destinations will be reachable from extension 2002. Test your prediction. From extension 2002, dial the following numbers. Only emergency and local numbers, should work. All other destinations should fail from extension 2002. The initial 0 is the PSTN access code:

112

0112

0-555-4444

00-606-555-4444 (This should not succeed.)

000-77-606-555-4444 (This should not succeed.)

Step 28

You have tested the route pattern (in partition P_Local) for local calls. The CSS_Local_only CSS is used only for testing. Route patterns in different partitions can be tested by changing the CSS that is assigned to the line.

Step 29

Now test the route pattern for national calls. This is in a different partition that is accessed only by the CSS_National_only CSS. Change the line CSS for extension 2002 to the following, and save and apply the configuration:

Calling Search Space: **CSS_National_only**

Step 30

Verify that only national calls are reachable from extension 2002. Dial the numbers that you tested earlier in this task. Emergency and national numbers, should work. All other destinations should fail from extension 2002:

112

0112

0-555-4444 (This should not succeed.)

0-0-606-555-4444

000-77-606-555-4444 (This should not succeed.)

You have now tested both the new route patterns for local and national calls in different partitions.

Step 31

Change the line CSS for extension 2002 to **CSS_Block_National**.

Step 32

From HQ Phone 2, place a test call to 112 (Emergency). Does this work? If not, explain why.

Step 33

From HQ Phone 2, place a test call to 00-606-555-4444 (National). Does this work? If not, explain why. Why is no reorder tone played?

Step 34

From HQ Phone 2, place a test call to 0-555-4444 (Local). Does this work? If not, explain why.

Step 35

From HQ Phone 2, place a test call to 000-77-606-555-4444 (International). Does this work? If not, explain why.

Note:Using the CSS_Block_National calling search space, only local and emergency calls are successful. National calls are blocked and no reorder tone would be provided since the route pattern is selected for "No Error" in the Block this pattern radio button. International calls are not successful since the International partition is not included in the CSS_Block_National calling search space.

Test Route Patterns for HQ Phone 1

In this section, you will test the route patterns that you added.

Step 36

Navigate to **Device > Phone** and click **Find**. Choose **HQ Phone 1** and modify Line 1 (2001) and set its CSS to **CSS_Local_National**.

Step 37

From HQ Phone 1, place a test call to 112 (Emergency). Does this work? If not, explain why.

Step 38

From HQ Phone 1, place a test call to 00-606-555-4444 (National). Does this work? If not, explain why.

Step 39

From HQ Phone 1, place a test call to 0-555-4444 (Local). Does this work? If not, explain why.

Step 40

From HQ Phone 1 place a test call to 000-77-606-555-4444 (International). Does this work? If not, explain why.

Note: Using the CSS_Local_National calling search space, only local, national, and emergency calls are successful. International calls are not successful since the International partition is not included in the CSS_Local_National calling search space.

Activity Verification

You have completed this task when you attain these results:

New partitions and CSSs are added in Cisco Unified Communications Manager.

New route patterns have been added in Cisco Unified Communications Manager.

The route patterns are assigned to different partitions.

The CoS is modified for HQ Phone 2 to prevent international and national calls.

HQ Phone 1 can make emergency, local, and national calls.

Set Route Patterns Back to PSTN Partition

In this task, you will set the partition on the route patterns back to **pstn**.

Complete these steps:

Step 41

Navigate to **Call Routing > Route/Hunt > Route Pattern** and click **Find**.

Step 42

Check the check box for the route pattern **0.0[1-9]XXXXXXXXX** with a description of **Block national calls** and click **Delete Selected**. Click **OK i**n the pop-up window that appears.

Step 43

For the 0.[1-9]XXXXXX route pattern (local), change the partition to **pstn**.

Step 44

Click **Save** and then click **OK** in the two pop-up windows that appear.

Step 45

In the Related Links drop-down list that is prepopulated with Back to Find/List, click **Go**.

Step 46

For the 0.0[1-9]XXXXXXXXX route pattern (local), change the partition to **pstn**.

Step 47

Click **Save** and then click **OK** in the two pop-up windows that appear.

Step 48

In the Related Links drop-down menu that is prepopulated with Back to Find/List, click **Go**.

Step 49

For the 000.[1-9]XXXXXXXXXXX route pattern (local), change the partition to **pstn**.

Step 50

Click **Save** and then click **OK** in the two pop-up windows that appear.

Pattern ▲	Description	Partition
0.0[1-9]XXXXXXXXX	National Calls	pstn
0.[1-9]XXXXXX	Local Calls	pstn
000.[1-9]XXXXXXXXXXX	international	pstn
0112	Emergency	pstn
112	Emergency	pstn
2500	RP to CUC	devices

Activity Verification

You have completed this task when you attain this result:

The partition on the route patterns is set back to pstn.

LAB 4: Implement End Users

LAB 4: Implement End Users

Use Microsoft Active Directory for End-User Synchronization to Configure End Users in Cisco Unified Communications Manager

In this task, you will configure end users in Cisco Unified Communications Manager by configuring new users in the Microsoft Active Directory for end-user synchronization.

Complete these steps:

Step 1

From the classroom PC, access the Cisco Unified Communications Manager Administration web pages with a web browser. Open the following URL: **http://10.1.5.15/ccmadmin**.

Step 2

In preparation for the next hardware lab, where you will use the self-provisioning feature, you have to re-create the directory numbers (lines) of the users when you import the users from LDAP. The recreation only works, if the directory numbers do not exist at the time the users are imported from LDAP for the first time. Therefore, you have to first delete the existing lines: Navigate to **Call Routing > Directory Number**, select all entries, and click **Delete Selected**.

Step 3

Navigate to **User Management > End User** and click **Find**. Choose the two previously configured end users, **jdoe** and **jwhite**, and click **Delete Selected**. (Do *not* delete any other end users that may exist.)

Step 4

Open a Remote Desktop Connection to the LDAP server at 10.1.5.14.

Step 5

When prompted, enter the credentials of **administrator** with a password of **cicdpass1!**.

Step 6

Navigate to **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. The Active Directory Users and Computers window opens.

Step 7

Choose **ciscoclass.com > Users**. Right-click in the right window and choose **New > User**.

Step 8

Enter the following information and save:

First Name: **John**

Last Name: **Doe**

User Logon Name: **jdoe**

Click **Next**

Password: **cicdpass1!**

Uncheck the box: **User must change password at next logon**

Step 9

Click **Next** and then click **Finish**. Right-click the newly created user and click **Properties**. Then set the Telephone number to **5155552001** and click **OK**.

Step 10

Create another user, Jane White, with a login name of **jwhite** and a telephone number of **5155552002**.

Step 11

In Cisco Unified Communications Manager Serviceability, navigate to **Tools > Service Activation**.

Step 12

Choose **10.1.5.15—CUCM Voice/Video** from the Server drop-down list.

Step 13

Find and activate the **Cisco DirSync** service.

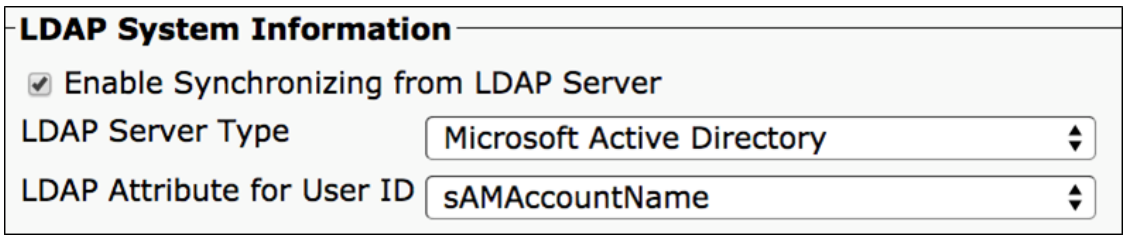
Step 14

In Cisco Unified Communications Manager Administration, navigate to **System > LDAP > LDAP System**. Set or verify the following parameters and **Save**.

Check the box: **Enable Synchronizing from LDAP Server**

LDAP Server Type: **Microsoft Active Directory**

LDAP Attribute for User ID: **sAMAccountName**



Step 15

Navigate to **System > LDAP > LDAP Directory**. Add a new LDAP Directory and configure the following parameters, leaving all other settings at default, and **Save**:

LDAP Configuration Name: **LDAP Server**

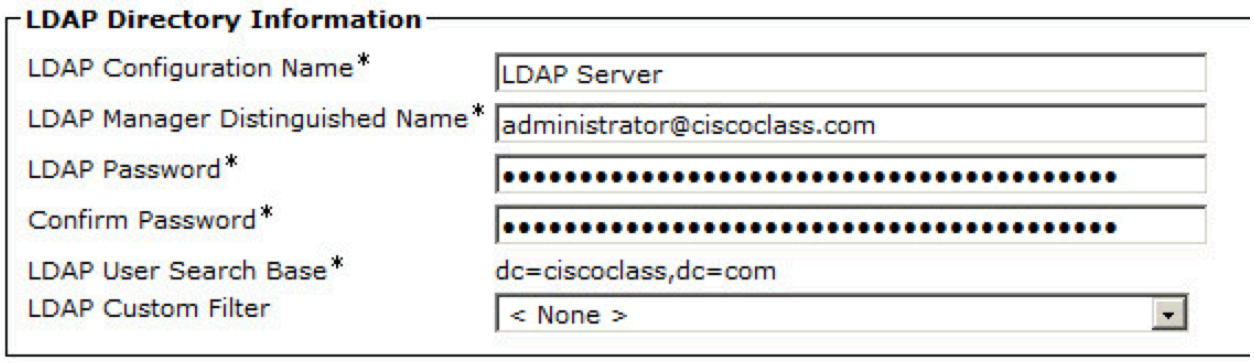
LDAP Manager Distinguished Name: **administrator@ciscoclass.com**

Note

In the lab, the Administrator account is used. In non-lab environments, the Microsoft Domain Administrator will provide you with a user and the relevant access rights. (read-only)

LDAP Password: **cicdpass1!**

LDAP User Search Base: **dc=ciscoclass, dc=com**



Note: In the lab, you are pointing to the root of the domain. This has the effect of synchronizing all users in the domain. In a production environment, you will usually point to more granular LDAP structures.

LDAP Custom Filter: **<None>**

Perform a Re-sync Every: **6 HOURS**

Access Control Group: **Standard CCM End Users**

Feature Group Template: **CICD FGT** (predefined)

Check the check box: **Apply mask to synced telephone numbers to create a new line for inserted users**

Mask: **2XXX**

Host Name or IP Address of Server: **10.1.5.14**

Step 16

Click **Perform Full Sync Now** to perform a complete LDAP synchronization. Refresh the screen repeatedly until the Cancel Sync Process link that is shown in the upper area of the screen changes to Perform Full Sync Now.

Step 17

Navigate to **User Management > End User** and click **Find**.

	User ID	First Name	Last Name	Department	Directory URI	User Status
	MediaSense		MediaSense			Active Local User
	jwhite	Jane	White			Active LDAP Synchronized User
	jdoe	John	Doe			Active LDAP Synchronized User
	student1	student1	student1			Active LDAP Synchronized User
	student2	student2	student2			Active LDAP Synchronized User

Step 18

Choose the user ID **jdoe** and verify that the user shows “Active LDAP Synchronized User”. (This may take a couple of minutes for the sync to complete).

Step 19

Notice that the self-service user ID is 2001 and the primary extension is 2001 in devices.

Note

The self-service user ID and primary extension settings are required for the upcoming Self Provisioning lab. The directory numbers have been created at the time when the users were imported. At this stage, however, the directory numbers are not associated with the phone.

Activity Verification

Complete this step to verify the task:

To verify LDAP synchronization, navigate to **User Management > End User** and click **Find**. The two previously configured users and two student IDs should be displayed with the status of “Active LDAP Synchronized User”.

Change User Settings in Cisco Unified Communications Manager

In this task, you will change end-user settings in Cisco Unified Communications Manager. Modify user configuration settings such as telephone number and user permissions.

Complete these steps:

Step 20

In Cisco Unified Communications Manager Administration, navigate to **User Management > End User** and click **Find**.

Step 21

Select **jdoe** as the user ID.

Step 22

Set the following parameters and save:

Password: **temppass1!**

Confirm Password: **temppass1!**

PIN: **131213**

Confirm PIN: **131213**

Step 23

From the Remote Desktop Connection to the LDAP server at 10.1.5.14, navigate to **Start > All Programs > Administrative Tools > Active Directory Users and Computers**, right-click the user **John Doe** and choose **Properties**.

Step 24

On the Organization Tab, populate the following fields:

Job Title: **Mad Scientist**

Department: **Management**

Step 25

In the Cisco Unified Communications Manager GUI, navigate to **System > LDAP > LDAP Directory** and select the **LDAP Server** entry. Then click on **Perform Full Sync Now**. Navigate to **User Management > End Users** and click **Find**. Choose the user **jdoe** and verify that the LDAP fields are populated in the user page.

Step 26

Sign out of the Administrative web interface.

Step 27

Open a browser connection to the Self Service Portal (http://10.1.5.15/ucmuser). Log in using the username **jdoe** and password **temppass1!** to verify that the credentials work properly (the password temppass1! was defined in the end user settings, not LDAP). If the credentials do not work, then verify that the user was added to the Standard CCM End Users Access Control Group.

Step 28

Sign out of the Self Service Portal.

Step 29

Log in to the Cisco Unified Communications Manager Administration, navigate to **LDAP > LDAP Authentication**. Enter the following information and save.

Check this box: **Use LDAP Authentication for End Users**

LDAP Manager Distinguished Name: **administrator@ciscoclass.com**

LDAP Password: **cicdpass1!**

LDAP User Search Base: **dc=ciscoclass, dc=com**

LDAP Server Information: **10.1.5.14**

Step 30

Navigate to the end user **jdoe** and verify that the Password field is gone.

Step 31

Sign out of the Administrative web interface.

Step 32

Log in again to the user web page using the user ID **jdoe**. Try the Cisco Unified Communications Manager password (**temppass1!**). This password does not work anymore. Use the Active Directory password **cicdpass1!** to log in.

Step 33

Sign out of the Self Service Portal.

Step 34

Log in to the Cisco Unified Communications Manager Administration, navigate to **LDAP > LDAP Custom Filter** and click **Add New**.

Step 35

Enter the following information to sync all users except usernames (last name) that start with **S** and save:

Filter Name: **NotS**

Filter: **(!(sn=s*))**

Note:The ! symbol in the above filter is used to change the logic to match anything that does not have a surname that starts with "s". The effect of this is that only end users that have surnames that start with "s" will be filtered.

Step 36

Navigate to the LDAP directory configuration and set the LDAP Custom Filter to **NotS** in the directory LDAP Server.

Step 37

Save and perform a full synchronization.

Step 38

Navigate to **User Management > End Users**. The user LDAP Status of student1 and student2 should be "Inactive LDAP Synchronized User".

Note

All inactive end users are deleted after 24 hours. The deletion process starts at 3:15 a.m. (0315). Use the LDAP filters carefully. For example, a wrong filter that is set on Friday might lead to issues (user loss)

over the weekend because all inactive users are gone, and therefore the user-specific settings are gone. In this case, the database must be restored.

Step 39

Remove the filter in the LDAP directory, perform another synchronization, and verify that the end-user status is active again for student1 and student2.

Activity Verification

You have completed this task when you attain these results:

End-user settings have changed on the LDAP server and are synchronized with Cisco Unified Communications Manager.

User permissions have been changed in Cisco Unified Communications Manager to allow jdoe access to the user web pages.

LDAP authentication is enabled and jdoe needs to enter the LDAP password when logging into the user web pages.

LDAP filters were tested and working. The LDAP filter cleanup task is done

LAB5: Implement Endpoints

LAB5: Implement Endpoints

Implement Endpoints

Complete this lab activity to practice what you learned in the related module.

Upon completing this guided lab, you will be able to:

Configure the Self-Provisioning IVR Service

Register IP phones with Cisco Unified Communications Manager using autoregistration

Self-provision registered phones

Register IP phones with Cisco Unified Communications Manager using Cisco Unified Communications Manager BAT

Request to initialize lab has been sent

Configure the Self-Provisioning IVR Service

In this lab, you will configure the Self-Provisioning IVR Service.

Complete these steps:

Step 1

Create a CTI Route Point that will be used to access the Self-Provisioning IVR service. In Cisco Unified Communications Manager, go to **Device > CTI Route Point** and click **Add New**.

Step 2

Configure the following fields on the CTI Route Point Configuration page and leave all other settings at their defaults:

Device Name: **SelfProv_RP**

Description: **Self Provisioning RP**

Device Pool: **Default**

Step 3

Click **Save**.

Step 4

After the new Route Point is saved, click the **Line (1)** link at the bottom of the page.

Step 5

Configure the following fields on the Directory Number Configuration, leaving all other settings at default:

Directory Number: **5000**

Route Partition: **Devices**

Description: **Pilot for Self Provisioning IVR Service**

Step 6

Click **Save**.

Step 7

Create an Application User that will be associated with the CTI Route Point that you just created. This application user will also be referenced on the Self Provisioning page later in the lab. Go to **User Management > Application User** and click **Add New**.

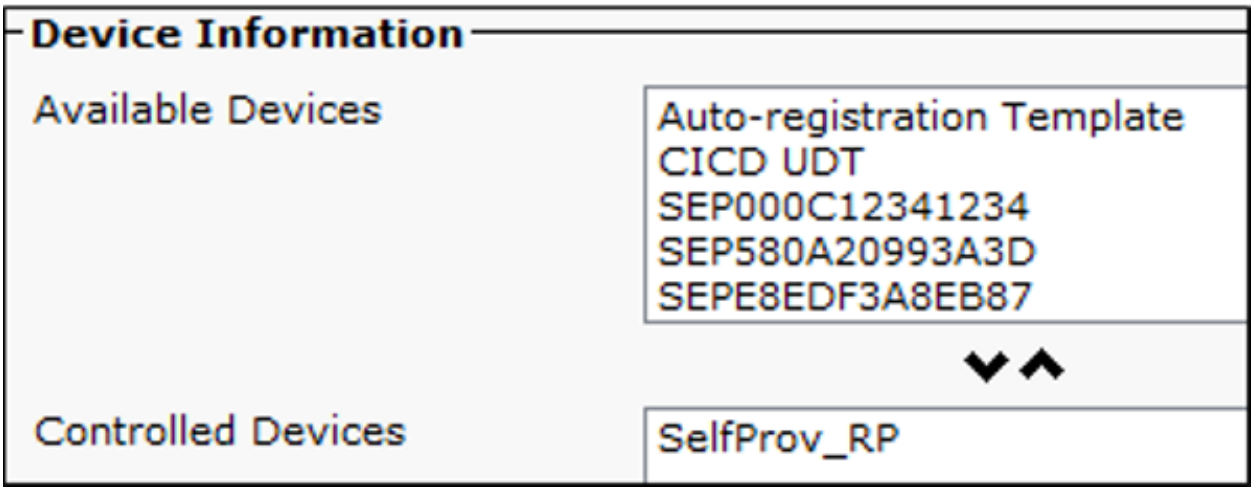
Step 8

Define the Application User with the following fields and associations:

User ID: **SelfProv**

Password: **cicdpass1!**

Controlled Device: **SelfProv_RP** (move from Available Devices section to Controlled Devices section)



Permission Information Group: **Standard CTI Enabled** (Click **Add to Access Control Group**.)

Step 9

Click **Save**.

Step 10

Navigate to the **Cisco Unified Serviceability** page in the upper-right corner of the Cisco Unified Communications Manager Administration GUI and click **Go**.

Step 11

Go to **Tools > Service Activation** and then choose **10.1.5.15 – CUCM Voice/Video** from the Server drop-down list.

Step 12

Check the **Self Provisioning IVR** service check box and click **Save**.

Step 13

Navigate to the **Cisco Unified CM Administration** page in the upper-right corner of the web page and click **Go**.

Step 14

To navigate to the Self Provisioning configuration, choose **User Management > Self-Provisioning**.

Step 15

On the Self Provisioning page, set the following values and click **Save**.

No Authentication Required radio button: **selected**

CTI Route Point: **SelfProv_RP**

Application User: **SelfProv**

Step 16

On the pop-up window, choose **Save and Restart Now**.

Activity Verification

You will verify that the Self Provisioning service has been configured correctly in Task 3.

Add a New Phone in Cisco Unified Communications Manager Using Autoregistration

In this task, you will register IP phones with Cisco Unified Communications Manager using autoregistration. First, remove all IP phones, and then add them again via autoconfiguration, using a Device Pool. New IP phones that are added via autoregistration will have restricted access. Manual changes will be required to permit full access to the IP phones.

Complete these steps:

Step 17

To begin the configuration of the Cisco Unified Communications Manager server for autoregistration, in Cisco Unified Communications Manager Administration, go to **System > Cisco Unified CM** and click **Find**.

Step 18

Choose **CM_CUCM** and configure the following settings:

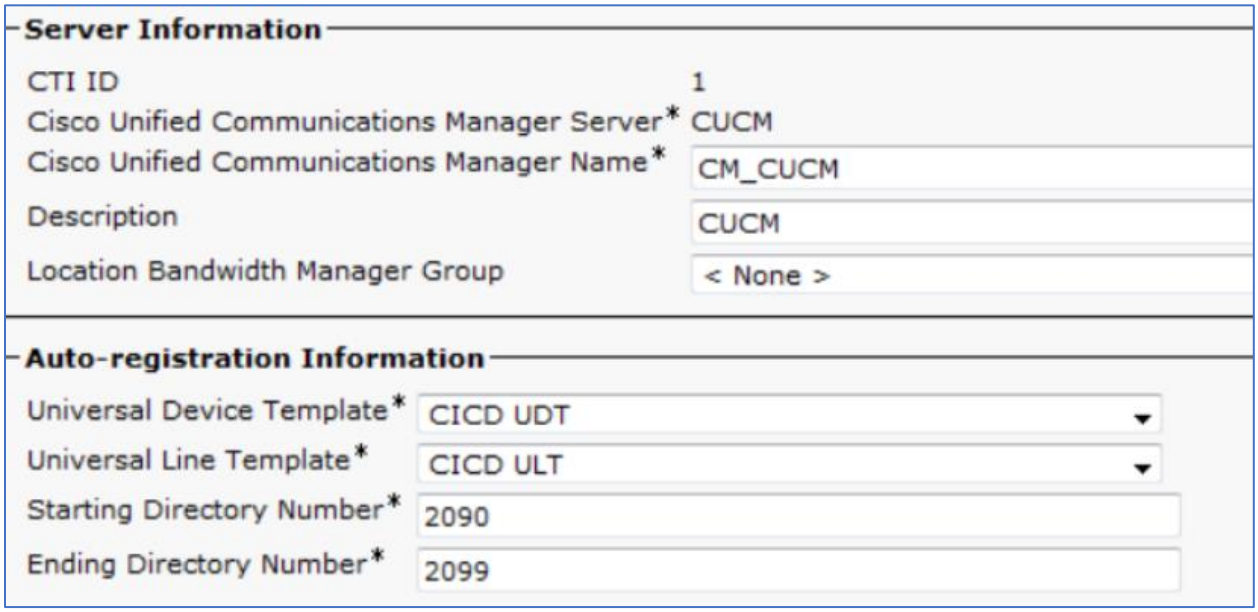
Universal Device Template: **CICD UDT** (the UDT was predefined by the instructor)

Universal Line Template: **CICD ULT** (the ULT was predefined by the instructor)

Ending Directory Number: **2099** (You modify the ending number first because Cisco Unified Communications Manager will check whether the starting number is lower than the ending number.)

Starting Directory Number: **2090** (Click **OK** in the pop-up window.)

Auto-registration Disabled on this Cisco Unified Communications Manager check box: This check box should have been unchecked automatically when Cisco Unified Communications Manager sees different values in the starting and ending directory number fields.



Step 19

Click **Save** and click **Apply Config**.

Step 20

To prepare to delete all IP phones from Cisco Unified Communications Manager, go to **Device > Phone** and click **Find**.

Step 21

Check the check boxes to the left of all the IP phones and click **Delete Selected**. Click **OK**.

Step 22

Watch the display as the HQ phones reset.

Step 23

The HQ phones will register using the autoregistration parameters. Verify that the directory numbers on the HQ phones are in the autoregistration range 2090 to 2099.

Step 24

Place test calls to the other HQ phone, and the PSTN to verify that calls succeed.

Activity Verification

You have completed this task when you attain this result:

The new IP phones have registered with Cisco Unified Communications Manager via autoregistration.

Use the Self-Provisioning IVR Service on Autoregistered Phones

In this task, you will self-provision the two autoregistered phones based on the LDAP telephone number on the end users that were imported.

Complete these steps:

Step 25

From HQ Phone 1 (which should have a DN of 2090 or 2091) dial **5000**, which is the DN for the Self Provisioning IVR Service.

Step 26

When prompted, enter the Self Provisioning ID of **2001**# followed by another #.

Note:The end user Self Provisioning ID was created during the "Configure the Self-Provisioning IVR Service" task. We will not be using authentication for Self Provisioning in this lab, although it is strongly recommended.

Step 27

On a hardware phone, you would hear confirmation that the phone will now provision and then it will reboot. With our IP Phone instances, you should see the phone re-register.

Step 28

After the reboot, the phone should now have a DN of 2001.

Step 29

From HQ Phone 2 (which should have a DN of 2090 or 2091), dial **5000**, which is the DN for the Self Provisioning IVR Service.

Step 30

When prompted, enter the Self Provisioning ID of **2002**# followed by another #.

Step 31

After the reboot, the phone should now have a DN of 2002.

Activity Verification

You have completed this task when you attain this result:

HQ Phone 1 has a DN of 2001 and HQ Phone 2 has a DN of 2002.

You have added a new IP phone in Cisco Unified Communications Manager using Self Provisioning.

Add a New Phone in Cisco Unified Communications Manager Using the Cisco Unified Communications Manager BAT

In this task, you will register an IP phone using the Cisco Unified Communications Manager BAT. You will also export an existing IP phone configuration to a text file and modify the text file to add a new IP phone. Finally, you will use the BR Phone as a new IP phone in Cisco Unified Communications Manager.

Complete these steps:

Step 32

In Cisco Unified Communications Manager Serviceability, navigate to **Tools Service Activation** and activate the **Cisco Bulk Provisioning Service**.

Step 33

To export IP phone configuration to a file, from Cisco Unified Communications Manager Administration, go to **Bulk Administration > Phones > Export Phones > Specific Details**.

Step 34

Enter the following information and then click **Find**:

Find Phones where: **Directory Number**

Begins with: **2001**

Step 35

One of the two phones should be displayed. Click **Next**.

Step 36

Enter the following information and then click **Submit**:

Filename: **Export2001**

File Format: **Default Phone Format**

Check this box: **Run Immediately**, then click **Submit**

Step 37

Go to **Bulk Administration > Job Scheduler** and click **Find**. Look in the Description field for the Export Configuration. The Status field will show completed when the job is finished.

Step 38

Navigate to **Bulk Administration > Upload/Download Files** and click **Find**.

Step 39

Choose the **Export2001** text file (the filename will include time and date information) and click **Download Selected**. Save the file to the PC Desktop.

Step 40

On the classroom PC, copy the file and name it **batphone.txt** as a backup before editing the contents.

Step 41

Use WordPad to open **batphone.txt**. Using Notepad may not display the content correctly.

Note

Be careful when editing the file. Spaces and commas may change the meaning of some of the fields.

Step 42

In WordPad, turn off word wrap. This will show two lines: the first line defines the fields and the second line is the exported details.

```
MAC ADDRESS,DESCRIPTION,LOCATION,DIRECTORY NUMBER 1,DISPLAY 1,LINE TEXT LABEL 1,
SEP580A20993A3D,AUTO 2001,Hub_None,2001,,2001,,,,,,,
```

Step 43

In the file, replace the following values in the text file and then save it:

MAC ADDRESS: **SEP000c12341234** (this is not a real device in the lab)

DESCRIPTION: **Fake BAT Phone**

DIRECTORY NUMBER 1: **2020**

LINE TEXT LABEL: **Fake BAT Phone**

```
MAC ADDRESS,DESCRIPTION,LOCATION,DIRECTORY NUMBER 1,DISPLAY 1,LINE TEXT LABEL 1,
SEP000c12341234,Fake BAT Phone,Hub_None,2020,,Fake BAT Phone,,,,,,,
```

Step 44

In Cisco Unified Communications Manager Administration, go to **Bulk Administration > Upload/Download Files**.

Step 45

Click **Add New** and enter the following:

File: Browse to locate the **batphone.txt** on the PC Desktop

Select The Target: **Phones**

Select Transaction Type: **Insert Phones – Specific Details**

Check this box: **Overwrite File if it exits**

Step 46

Click **Save**.

Step 47

Verify that the screen refreshes with “Upload successful.”

Step 48

Go to **Bulk Administration > Upload/Download Files** and verify that the batphone.txt is in the list.

Step 49

To create a new Phone Template, go to **Bulk Administration > Phones > Phone Template** and click **AddNew**.

Step 50

From the Phone Type drop-down list, choose **Cisco 9971** and click **Next**.

Step 51

Enter the following and click **Save**:

Template Name: **MyTemplate**

Device Pool: **Default**

Phone Button Template: **Standard 9971 SIP**

Calling Search Space: **pstn**

Device Security Profile: **Cisco 9971 – Standard SIP Non-Secure Profile**

SIP Profile: **Standard SIP Profile**

Step 52

Select **Line 1** of the template. Enter the following and click **Save**:

Line template Name: **LineTemplate**

Partition: **devices**

Calling Search Space: **CSS_Local_National**

Step 53

Go to **Bulk Administration > Phones > Validate Phones**.

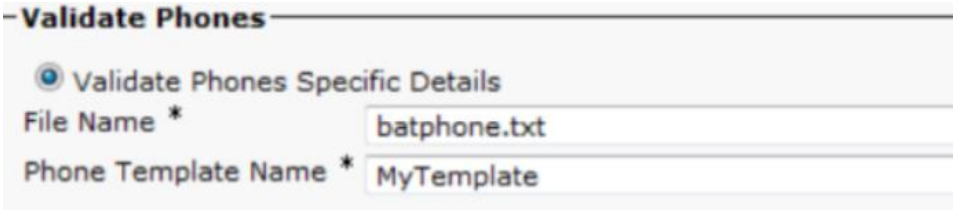
Step 54

Enter the following and click **Submit**:

Check this box: **Validate Phones Specific Details**

Filename: **batphone.txt**

Phone Template Name: **MyTemplate**

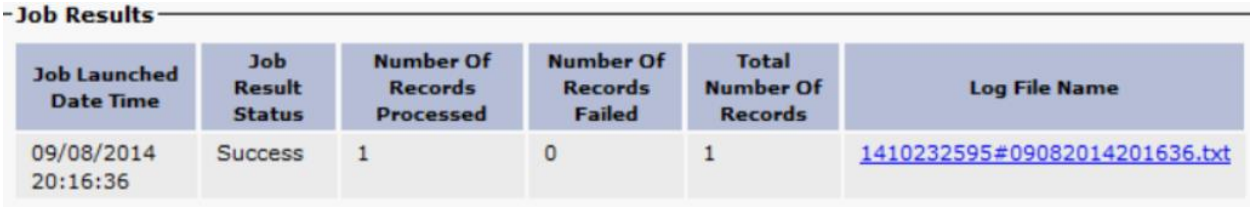


Step 55

Go to **Bulk Administration > Job Scheduler** and click **Find**. Look in the Description field for the Validate Phones job.

Step 56

Click the Job ID to view the job result. Look for any failure counters. In the Job results section, you should see the following:



Step 57

Click the Log File Name to view the log. Look for the following message:

******** NO ERROR FOUND ********

Step 58

Close the window. Fix any errors in the log before continuing.

Step 59

Go to **Bulk Administration > Phones > Insert Phones**.

Step 60

Enter the following:

Check this radio button: **Insert Phones Specific Details**

File Name: **batphone.txt**

Phone Template Name: **MyTemplate**

Check this box: **Override the existing configuration**

Check this box: **Run Immediate**

Step 61

Click **View File** to the right of Insert Phones Specific Details. Check your file content. Click **Close** when done.

Step 62

Click **View Sample File** and look at the file format. Click **Close** when done.

Step 63

Click **Submit**. Verify that the screen refreshes with "Add Successful."

Step 64

Go to **Bulk Administration > Job Scheduler** and click **Find**. Look in the Description field for Insert Phones and the Status field for Completed.

Step 65

Click the Job ID to view the job result. Look for any failure counters. You should see the following:

Job Results

Job Launched Date Time	Job Result Status	Number Of Records Processed	Number Of Records Failed	Total Number Of Records	Log File Name
09/08/2014 20:20:17	Success	1	0	1	1410232816#09082014202016.txt

Step 66

Click the Log File Name to view the log. Look for the following message:

******** NO ERROR FOUND ********

Result Summary :

INSERT for 1 PHONES passed.

INSERT for 0 PHONES failed.

Step 67

To verify that the new IP phone is added in Cisco Unified Communications Manager, go to **Device > Phone**.

Step 68

Enter the following information and click **Find**:

Find Phones where: **Directory Number**

Begins with: **2020**

Step 69

The new IP phone configuration should be displayed. View the device and line configuration of the new IP Phone. Check that the following are configured correctly (as shown previously):

Line 1

Partitions

CSS

Activity Verification

You have completed this task when you attain these results:

You have exported Cisco Unified Communications Manager IP phone configuration parameters to a text file using the Cisco Unified Communications Manager BAT.

You have added a new IP phone in Cisco Unified Communications Manager using the Cisco Unified Communications Manager BAT.

LAB6: Enable Telephony Features

Lab6: Enable Telephony Features

Upon completing this guided lab, you will be able to:

Configure Group Pickup in Cisco Unified Communications Manager

Configure Directed Call Park in Cisco Unified Communications Manager

Configure intercom functionality in Cisco Unified Communications Manager

Configure IP Phones for BLF Speed Dials

Request to initialize lab has been sent

Configure Group Pickup for the HQ Phones

In this task, you will configure a pickup group for both HQ phones. You will modify the phone button for Call Pickup functionality and add the softkey buttons to the on-hook call state. The pickup group will use the directory number 2801 and the directory numbers 2001 and 2002 will be added to the pickup group.

Complete these steps:

Step 1

Navigate to **Call Routing > Call Pickup Group** and click **Add New**.

Step 2

In the window that appears, enter the following values:

Call Pickup Group Name: **HQ-Pickup**

Call Pickup Group Number: **2801**

Description: **HQ Pickup Group**

Partition: **devices**

Step 3

From the Call Pickup Group Notification Policy drop-down list, choose **Audio and Visual Alert**. This enables an audible and visual notification on the devices in a pickup group.

Step 4

Check the **Calling Party Information** and **Called Party Information** check boxes.

Step 5

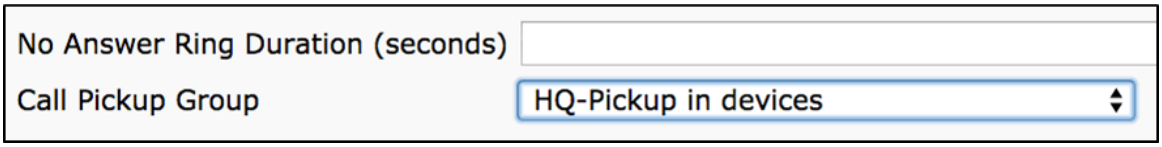
Click **Save**.

Step 6

Navigate to **Device > Phone** and search for HQ Phone 1.

Step 7

Choose the directory number **2001**. Remove the Forward No Answer Internal and External destinations and from the Call Pickup Group drop-down list choose **HQ-Pickup**. Save and apply the changes.



Step 8

Repeat Step 7 for HQ Phone 2 with the directory number 2002. Both directory numbers are now in the same Call Pickup Group.

Configure and Apply a Phone Button Template to Support Group Pickup

Complete these steps:

Step 9

Navigate to **Device > Device Settings > Phone Button Template**, choose the **Standard 7965 SCCP** template (which is on the second page) and click **Copy**. In contrast to softkey templates, device button templates are device specific.

Step 10

Enter **CICD PBT 7965 SCCP** for the name of the phone button template.

Step 11

Configure the following layout:

Button 1: **Line** (this button is not editable)

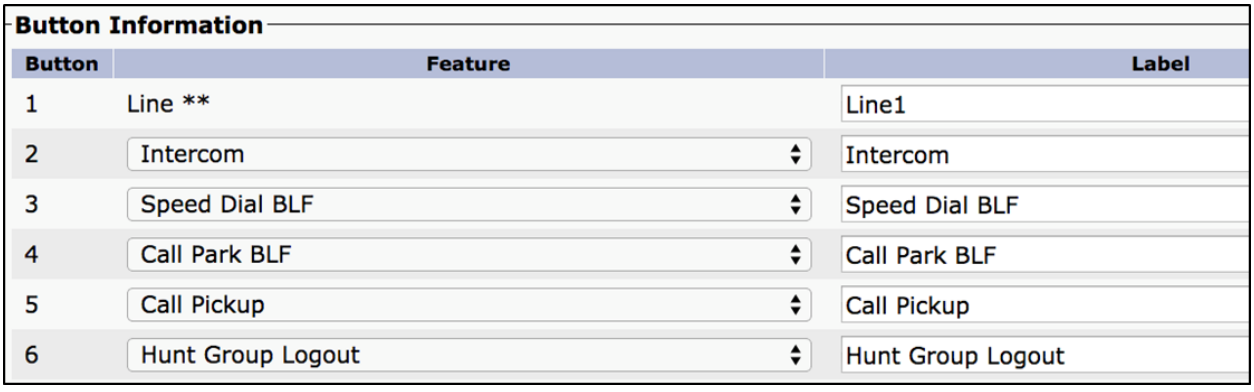
Button 2: **Intercom**

Button 3: **Speed Dial BLF**

Button 4: **Call Park BLF**

Button 5: **Call Pickup**

Button 6: **Hunt Group Logout**



Step 12

Save the configuration.

Step 13

Navigate to **Device > Phone** and choose the **HQ Phone 1**.

Step 14

Choose **CICD PBT 7965 SCCP** from the Phone Button Template drop-down list, and then save and apply the configuration.

Step 15

Verify on the display of HQ Phone 1 that the new phone button template was applied to the IP phone. (When using the IP Softphone instance, the buttons will not display the feature name properly until they are configured in the upcoming steps).

Step 16

Repeat last 3 steps to assign the same Phone Button Template to HQ Phone 2 and verify the configuration.

Step 17

Configure another 7965 SCCP IP Phone in Cisco Unified Communications Manager. Configure it the same as the previous phones were configured, but use the MAC address of **555555555555** (The number 5 12 times) and a directory number of **2005**. On the Phones PC, make sure to add it as instance 4 and as a 7965. Use 10.1.5.15 as the TFTP server.

Activity Verification

Complete the following steps to verify the configuration:

Test the Pickup feature. The softkey includes the Group Pickup feature and the Phone Button Template includes the Pickup feature. Call from the Test Phone to the directory number 2001.

Watch HQ Phone 2 and wait for the default timer for Call Pickup notifications (6 seconds). Watch the display for the visual Call Pickup notification. On HQ Phone 2, Press **New Call>More>>** then click **Pickup** and answer the call.

Configure Directed Call Park

In this task, you will configure the Directed Call Park feature for the HQ phones. Use the number 2811 as the call park number and use 2001 as the reversion number. Set the revision timer to 30 seconds and configure a Call Park BLF on HQ Phone 2.

Complete these steps:

Step 18

Navigate to **Call Routing > Directed Call Park** and click **Add New**.

Step 19

In the window that appears, enter the following values:

Number: **2811**

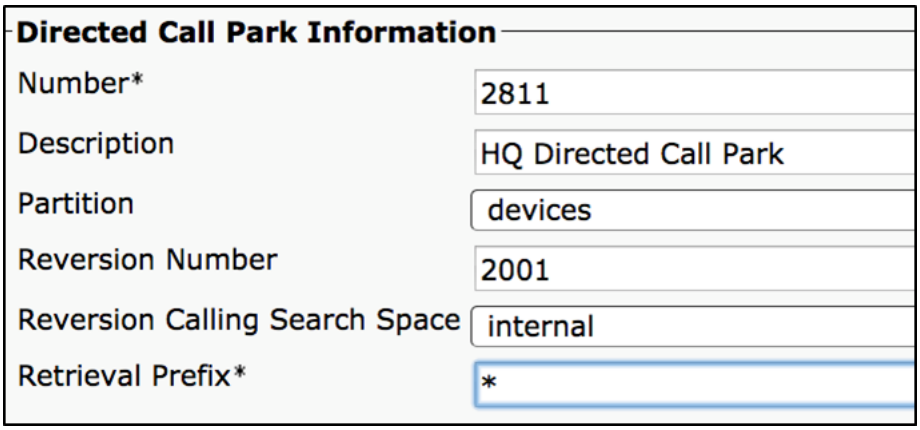
Description: **HQ Directed Call Park**

Partition: **devices**

Reversion Number: **2001**

Reversion Calling Search Space: **internal**

Retrieval Prefix: *



Step 20

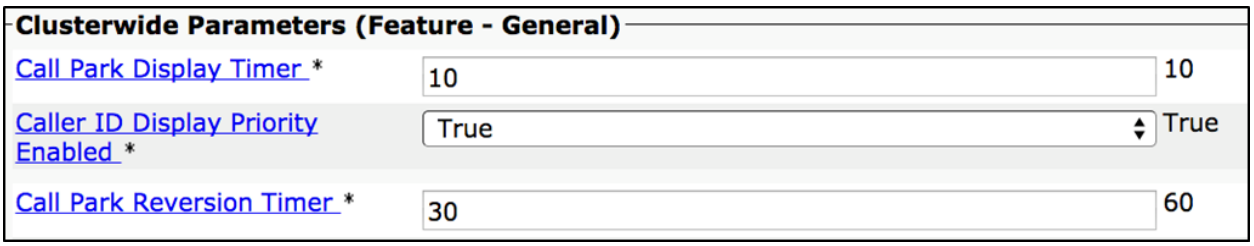
Click the **Save** button.

Step 21

Navigate to **System > Service Parameter** and choose the **10.1.5.15—CUCM Voice/Video** server. Choose the **Cisco CallManager service**.

Step 22

Set the Call Park Reversion Timer to **30** seconds. Save the changes.



Step 23

Go to **Device > Phone**. Change the **Softkey Template** on both HQ Phone 1 and 2 to Standard User and reset the phones.

Step 24

From HQ Phone 1, call the directory number 2002 (HQ Phone 2). Answer the call on HQ Phone 2 and press the **Transfer** button. Transfer the call to 2811 and press the **Transfer** button again. Verify on HQ Phone 1 that the display shows the connected Call to Park Number. From HQ Phone 2, dial ***2811**. HQ Phone 2 is now connected again to HQ Phone 1.

Step 25

Now, test the reversion number and timer. Call from HQ Phone 2 the directory number 2001 (HQ Phone 1). Answer the call on HQ Phone 1 and press the **Transfer** button. Transfer the call to 2811 and press the **Transfer** button again. Verify on HQ Phone 2 that the display shows the connected Call to Park Number. Wait 30 seconds. The call should ring automatically again on extension 2001.

Activity Verification

You have completed this task when you attain this result:

Directed Call Park was configured and tested successfully.

Configure Intercom Functionality

In this task, you will create an intercom line for HQ Phone 1 and HQ Phone 2. The intercom partition name is Intercom Sales. Use the directory number 2101 for John Doe and 2102 for Jane White.

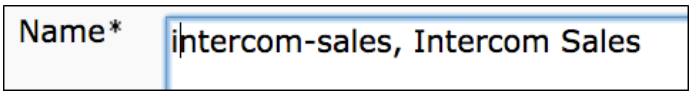
Complete these steps:

Step 26

Navigate to **Call Routing > Intercom > Intercom Route Partition** and click **Add New**.

Step 27

Use intercom-sales as the partition name and the description Intercom Sales. Enter the command in the following format: **intercom-sales, Intercom Sales**.



Step 28

Save the configuration.

Step 29

Navigate to **Call Routing > Intercom > Intercom Calling Search Spaces** and click **Find**.

Step 30

Verify that Cisco Unified Communications Manager created the necessary CSS. The name of the CSS is intercom-sales_GEN.

Step 31

Navigate to **Device > Phone** and search for HQ Phone 1.

Step 32

To create a new intercom directory number, click the **Intercom [1] – Add a new Intercom** link, which is on button 2.

Step 33

Use the following parameters for the intercom directory number and save the changes:

Intercom Directory Number: **2101**

Route Partition: **intercom-sales**

Description: **Intercom John Doe**

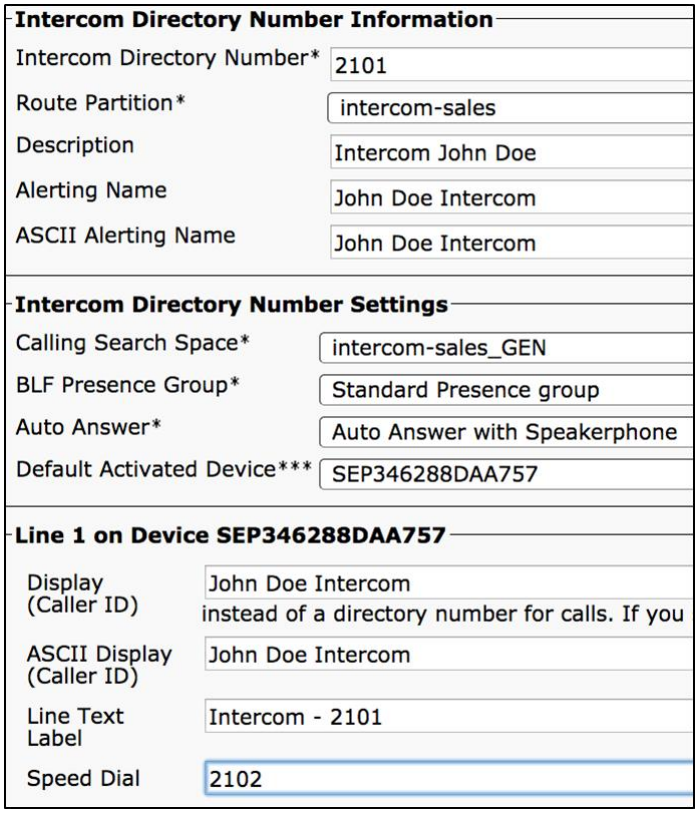
Alerting Name: **John Doe Intercom**

Calling Search Space: **intercom-sales_GEN**

Display (Caller ID): **John Doe Intercom**

Line Text Label: **Intercom - 2101**

Speed Dial: **2102**



Step 34

Navigate to **Device > Phone** and search for HQ Phone 2.

Step 35

Configure the intercom with the following values:

Intercom Directory Number: **2102**

Route Partition: **intercom-sales**

Description: **Intercom Jane White**

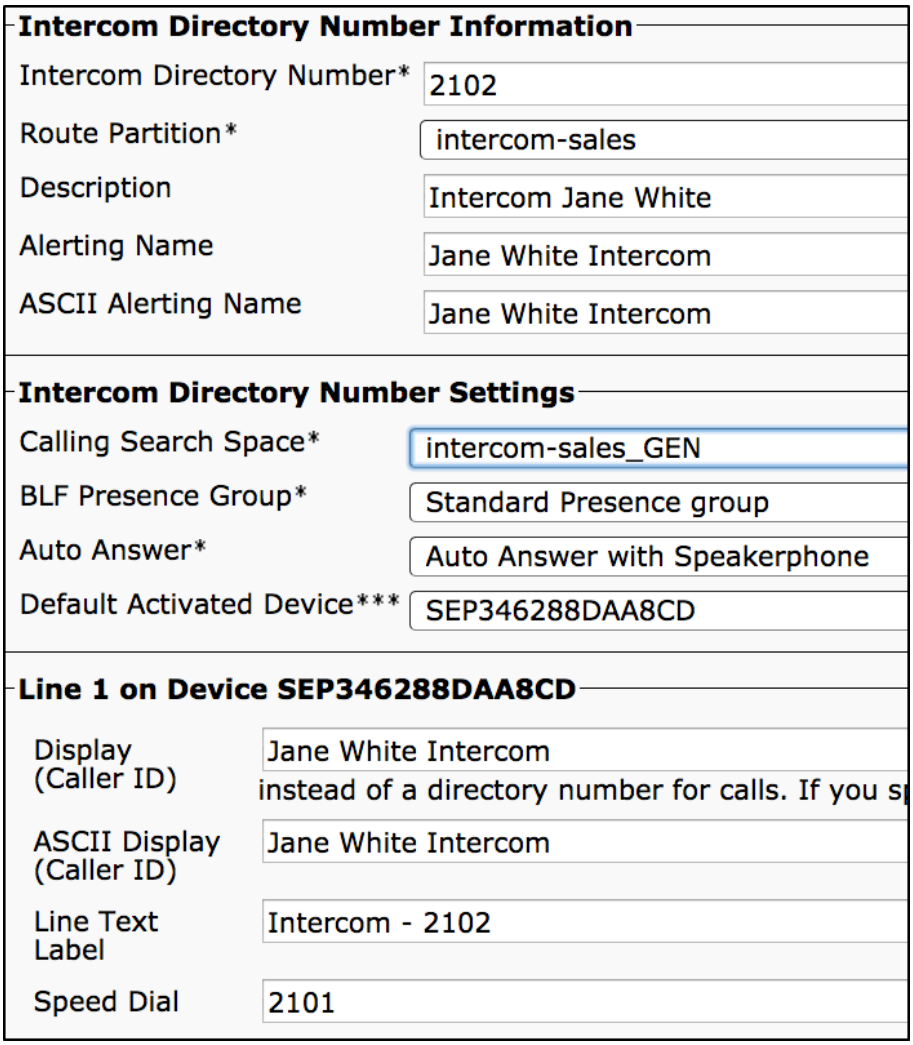
Alerting Name: **Jane White Intercom**

Calling Search Space: **intercom-sales_GEN**

Display (Caller ID): **Jane White Intercom**

Line Text Label: **Intercom - 2102**

Speed Dial: **2101**



Step 36

Click **Save** and verify that both intercom lines are shown on the IP phone displays.

Step 37

Test the intercom configuration. Intercom is typically used between an assistant and a manager. Call from the Test Phone to the directory number 2001 and answer the call.

Step 38

Press the **Intercom** button on HQ Phone 1.

Step 39

Verify that a one-way audio stream is open to HQ Phone 1 (This is difficult for students using the full remote setup because all phones share the same audio resources on your PC). HQ Phone 2 should show the one-way whisper symbol in the IP phone display. On HQ Phone 1, verify that the call to Test Phone 1 is still active (on hold – flashing red).

Step 40

Verify on the Test Phone that the call to HQ Phone 1 is on hold.

Activity Verification

You have completed this task when you attain this result:

Intercom was configured on HQ Phone 1 and 2 and a one-way intercom call was established.

Configure IP Phones for BLF Speed Dials

In this task, you will create a BLF-enabled speed dial on HQ Phone 1 and HQ Phone 2 so that HQ Phone 1 can monitor the HQ Phone 2 directory number and vice versa. The BLF-enabled speed dial on HQ Phone 2 should be configured to pick up calls from HQ Phone 1.

Complete these steps:

Step 41

Navigate to **Device > Phone** and choose **HQ Phone 1**.

Step 42

On button 3, click the **Add a new BLF SD** link.

Step 43

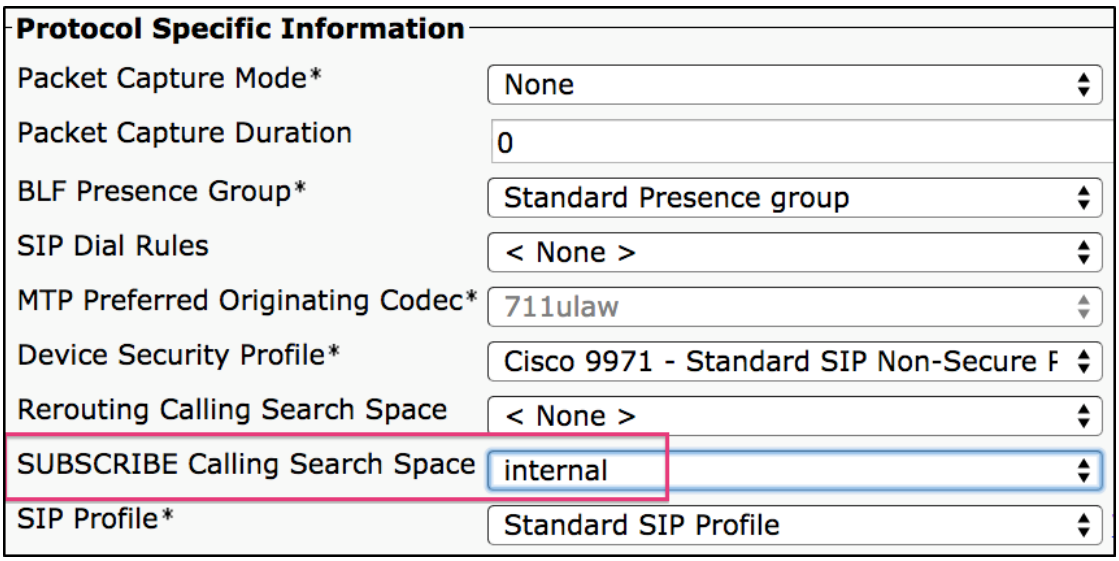
In the first row, choose **2002 in devices** from the Directory Number drop-down field.

Step 44

Enter **Jane White** as the label and save the changes.

Step 45

On HQ Phone 1, set the SUBSCRIBE Calling Search Space to **internal**.



Step 46

Save the changes and apply the configuration.

Step 47

Repeat Steps 1 through 6 for HQ Phone 2 and add a BLF SD for directory number 2001 (John Doe). In addition, check the **Call Pickup** check box when configuring the BLF-enabled speed dial.

Step 48

On HQ Phones 1 and 2, verify that both displays are showing the BLF Speed Dial. You should also see the status of the BLF destination.

Step 49

Test the configuration and call from the Test Phone to HQ Phone 1. Answer the call on HQ Phone 1. The light of the BLF button on HQ Phone 2 is now on (red).

Activity Verification

You have completed this task when you attain this result:

Both BLF-enabled speed dials are configured and shows the status as Busy when a call is in progress.

LAB7: Enable Mobility Features

LAB7: Enable Mobility Features

Upon completing this guided lab, you will be able to:

Change when calls to the remote destination ring

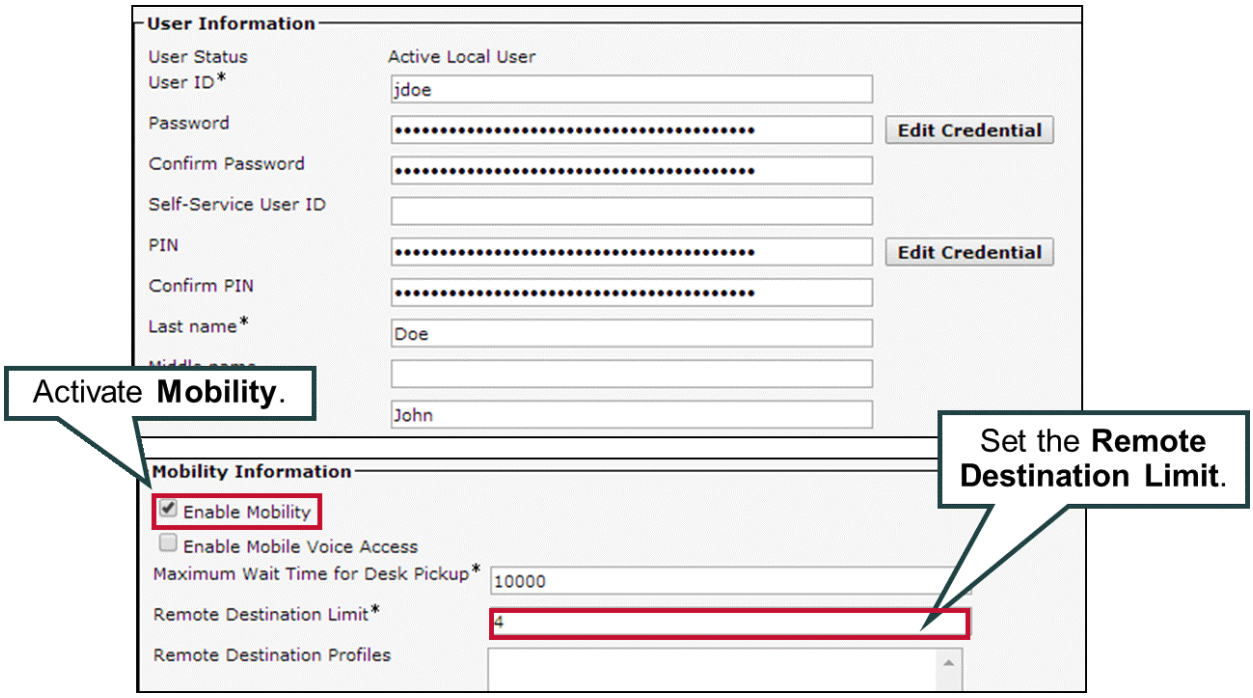
Configure the remote destination to ring longer

Prevent the remote destination from ringing when receiving calls from the branch

Request to initialize lab has been sent

Enable Mobility on the End User

Follow these steps to enable the end user jdoe for mobility:



Step 1

To configure end-user settings, navigate to **User Management > End User** and search for **jdoe**.

Step 2

Click **jdoe** to edit the settings for this user.

Step 3

In the window that appears, in the Mobility Information section, check the **Enable Mobility** check box and leave the Remote Destination Limit set to **4**, which is the default. Make sure that the Enable Mobile Voice Access is not checked.

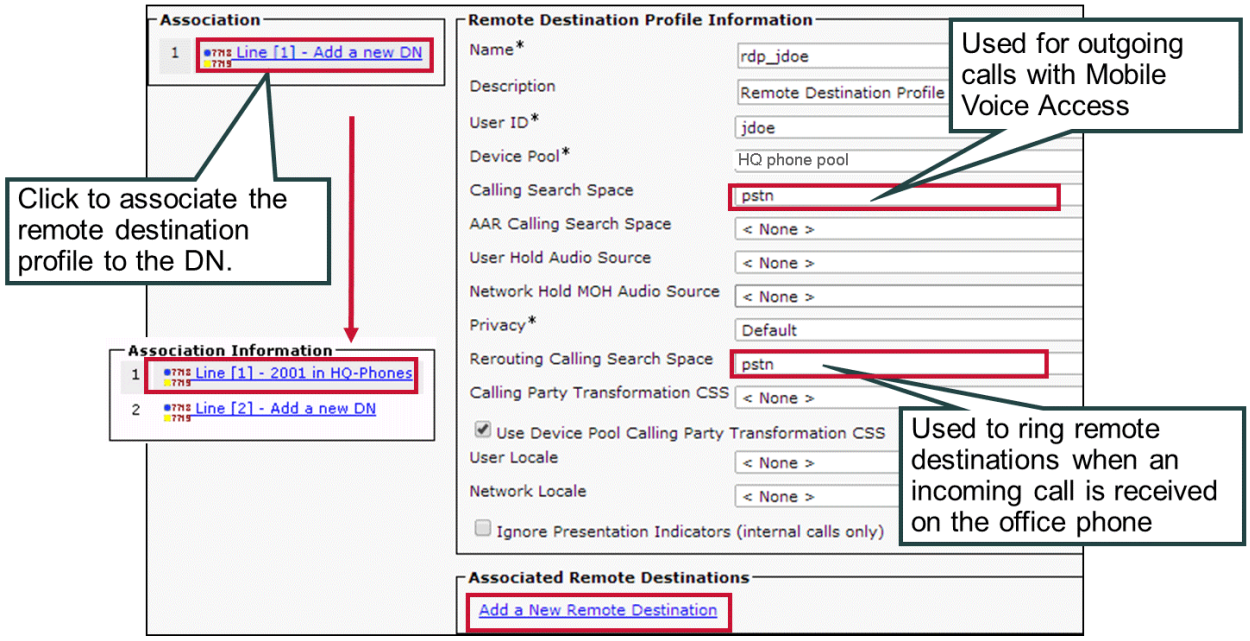
Step 4

Save the Changes.

Note: When the user was imported from LDAP, the configured Feature Group Template was configured to enable Mobility and Mobile Voice Access. By default, both would be disabled.

Create a Remote Destination Profile for the User

Follow these steps to create a Remote Destination profile for jdoe.



Step 5

Navigate to **Device > Device Settings > Remote Destination Profile**.

Step 6

Click **Add New** to create a new destination profile.

Step 7

Use the following values for the Remote Destination Profile:

Name: **rdp_jdoe**

Description: **Remote Destination Profile for jdoe**

User ID: **jdoe**

Device Pool: **Default**

Rerouting Calling Search Space: **pstn**

Step 8

Save the changes.

Step 9

Click **Line [1] – Add a new DN** to associate the Remote Destination Profile with the directory number.

Step 10

Enter **2001** as the directory number and choose **devices** as the route partition. The remaining settings will be taken from DN 2001.

Step 11

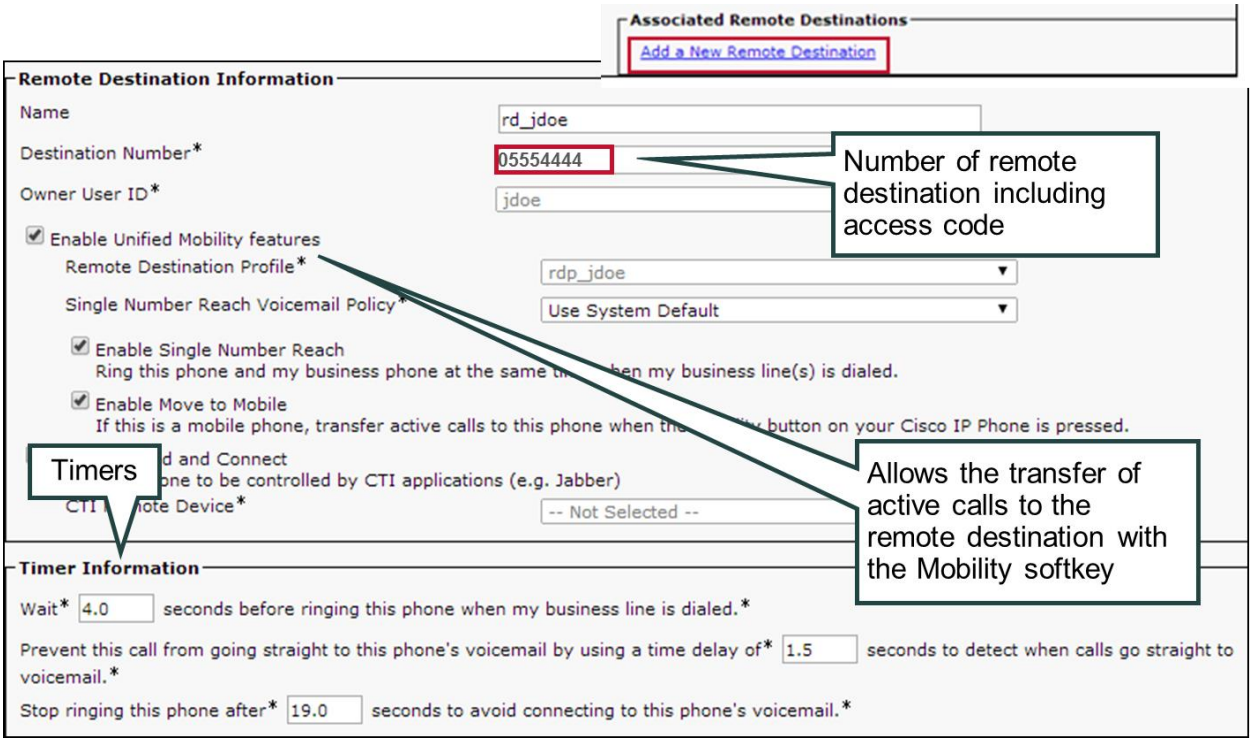
Click **Save** and click **Apply Config**.

Step 12

From the Related Links drop-down list, choose **Configure Device (rdp_jdoe)**.

Add Remote Destinations to a Remote Destination Profile

Follow these steps to add remote destinations to the remote destination profile that you created in Task 2.



Step 13

From the Remote Destination Profile Configuration window, click **Add a New Remote Destination** to configure the local line of the PSTN phone as the remote destination.

Step 14

Use the following values for the remote destination:

Name: **rd_jdoe**

Destination Number: **05554444** (including the access code 0)

Step 15

Verify that the following settings are present:

Enable Unified Mobility Features: Checked

Remote Destination Profile: rdp_jdoe (may be grayed out)

Enable Single Number Reach: Checked

Enable Move to Mobile: Checked

Step 16

Notice the default Timer Information section and leave these settings at their defaults.

Step 17

Save the configuration.

Step 18

At the Remote Destination Profile section on the left, check the Line Association check box and click Save.

Configure Service Parameters

Follow these steps to configure the service parameters:

Step 19

Navigate to **System > Service Parameters** and choose **CallManager Service**.

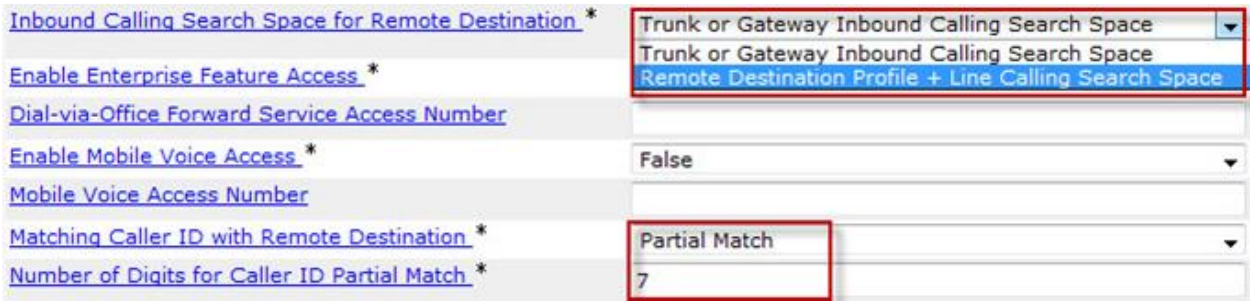
Step 20

In the section titled Clusterwide Parameters (System – Mobility), set the following values:

Inbound Calling Search Space for Remote Destinations: **Remote Destination Profile + Line Calling Search Space**

Matching Caller ID with Remote Destination: **Partial Match**

Number of Digits for Caller ID Partial Match: 7



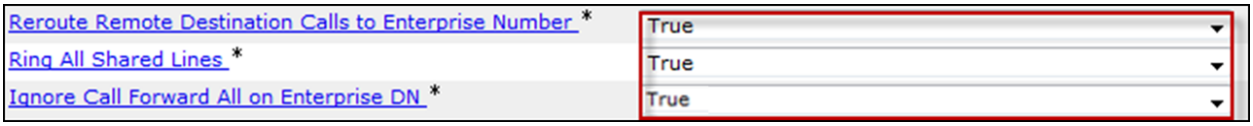
Step 21

In the section titled Clusterwide Parameters (Feature Reroute Remote Destination Calls to Enterprise Number), set the following values:

Reroute Remote Destination Calls to Enterprise Number: **True**

Ring All Shared Lines: **True**

Ignore Call Forward All on Enterprise DN: **True**



Activity Verification

You have completed this task when you attain this result:

Call HQ Phone 1 from 2002. The call should be extended to the PSTN Phone.

Change user password (John Doe) in Active Directory

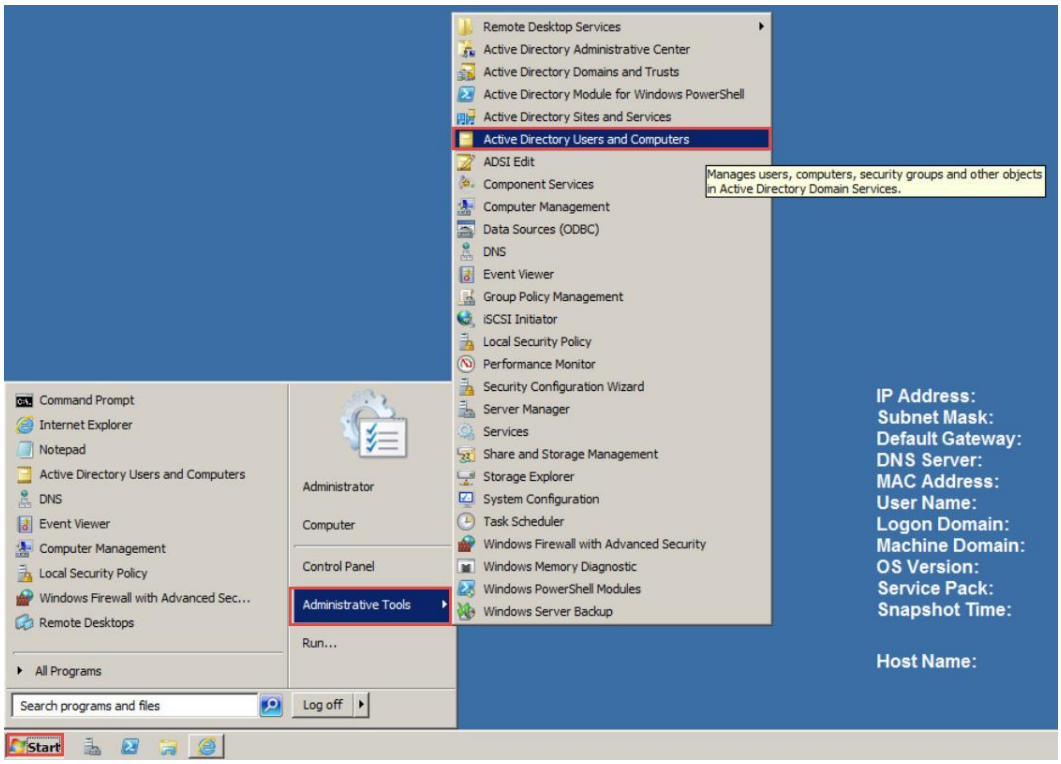
In this next few steps, you will change the password of the user (John Doe) in preparation for configuring mobility features.

Step 22

Log in to the Active Directory server (**DC-HQ**) using the username (**Administrator**) and password (**cicdpass1!**)

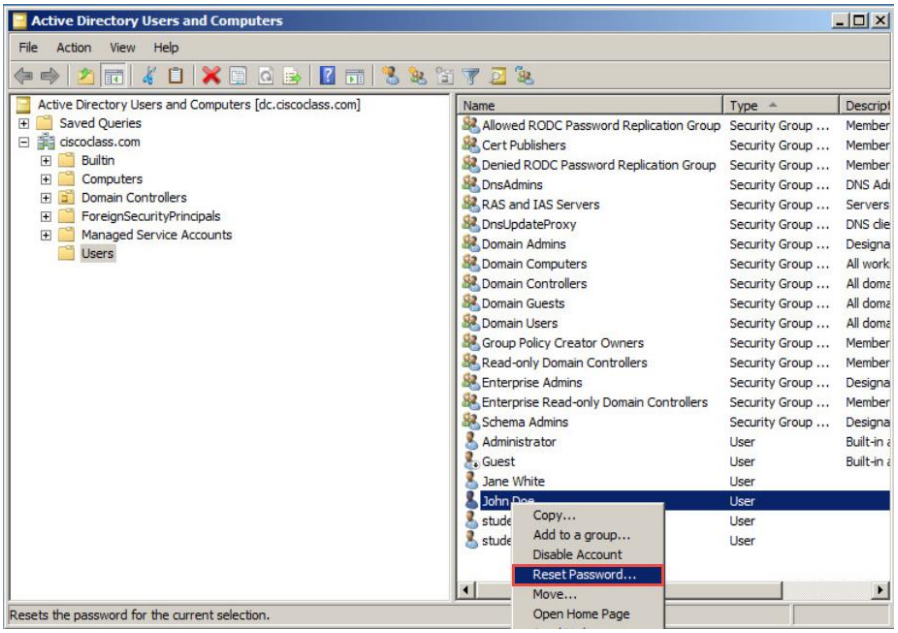
Step 23

Select **Start > Administrative Tools > Active Directory Users and Computers**



Step 24

In the Users folder, right click on user **John Doe** and select **Reset Password**.



Step 25

Enter the new password (**cicdpass1!**). Then, enter it once more to confirm.

Step 26

Uncheck the **User must change password at next logon** checkbox and click **OK**. Then, click **OK** once again on the popup window.

Step 27

Exit the Active directory server PC and continue with the lab.

Activity Verification

You have completed this task when you attain this result:

You have successfully changed the password of the user (John Doe) in Active Directory as described in the steps.

Change When Calls to the Remote Destination Ring

Scenario

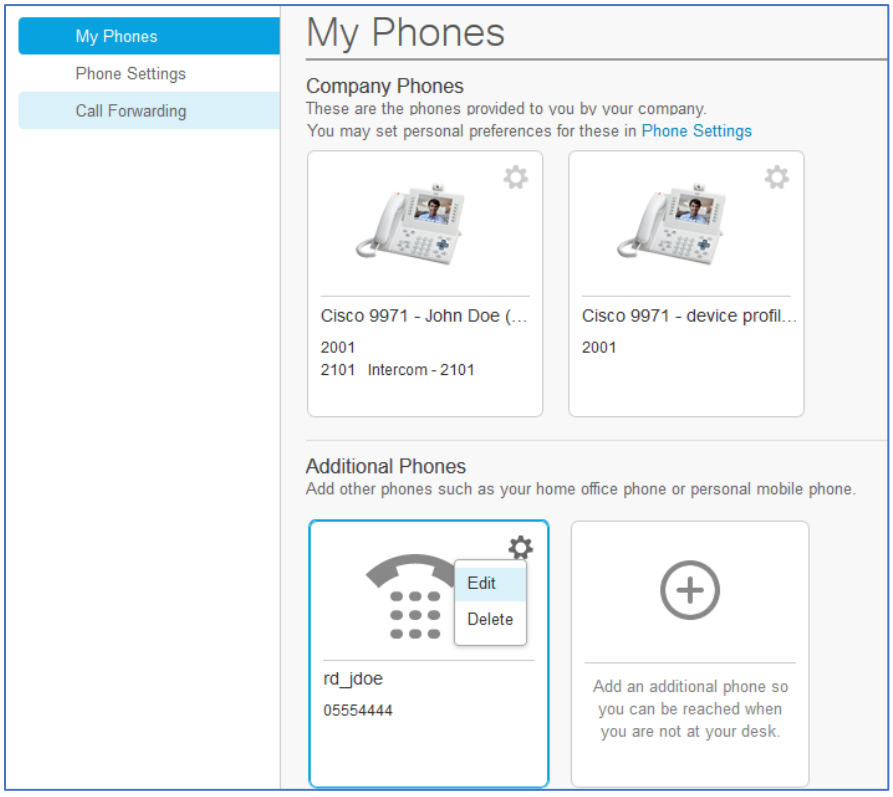
Configure Mobility for jdoe so that the previously configured remote destination only rings on Saturday and Sunday between 8:00 a.m. (0800) and 5:00 p.m. (1700) CET.

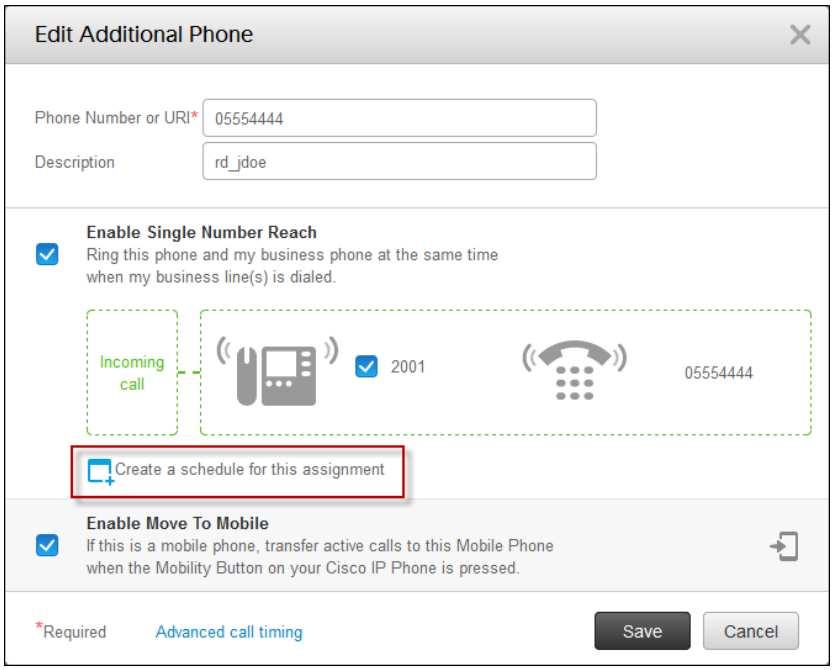
Step 28

Navigate to **https://10.1.5.15/ucmuser** and log in with the credentials of **jdoe/cicdpass1!**.

Step 29

Select the previously configured remote destination of rd_jdoe and edit the remote destination.



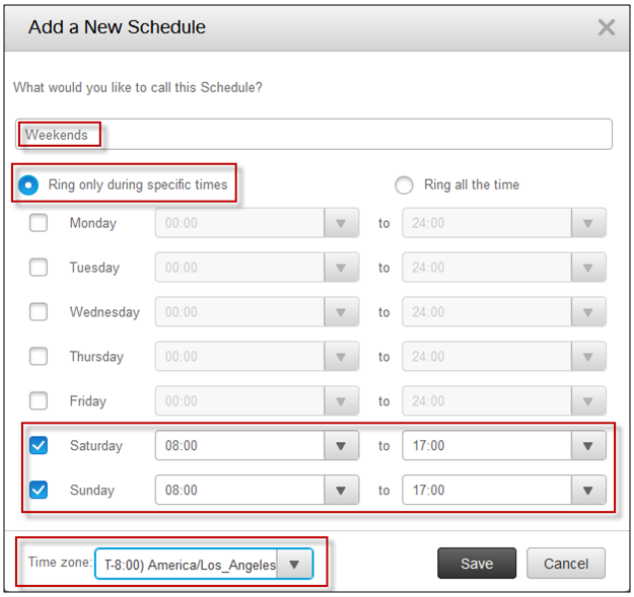


Step 30

Make a new schedule named **Weekend** and set it to only ring on Saturday and Sunday from 08:00 to 17:00 for both days.

Step 31

Set the timezone correctly for your location.



Step 32

Save the changes.

Step 33

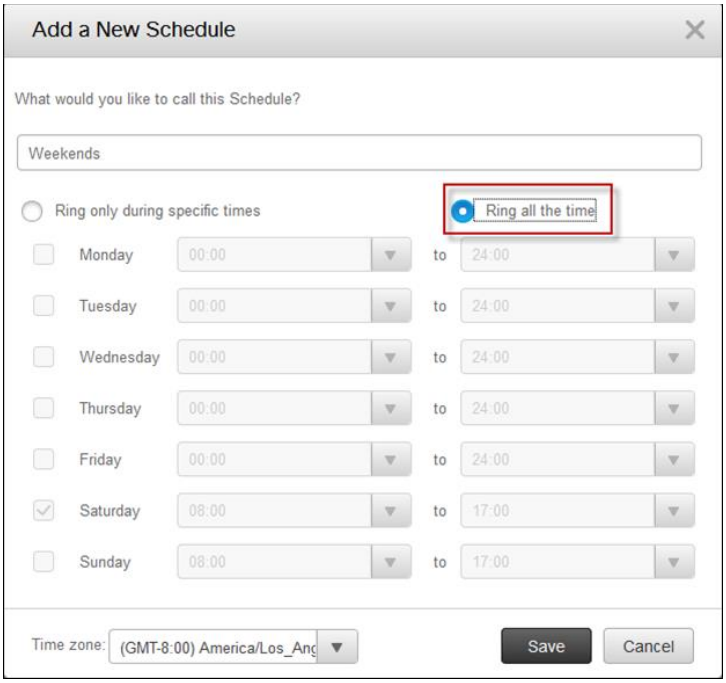
Test the ring schedule by calling directory number 2001 from HQ Phone 2.

Step 34

On the PSTN phone, verify that incoming calls to HQ Phone 1 do not ring at the local line.

Step 35

Under Configure Schedule, choose **All the time** and save the changes.



Step 36

Call the directory number 2001 again from HQ Phone 2. The PSTN phone on the local line should receive the incoming call again.

Activity Verification

You have completed this task when you attain this result:

The ring schedule was successfully enabled and disabled.

Configure the Remote Destination to Ring Longer

Scenario

The user jdoe complains that the remote destination rings for only a few seconds. Show jdoe how to make these changes using the Self Provisioning Tool. John Doe wants the remote destination to ring immediately and for up to 30 seconds.

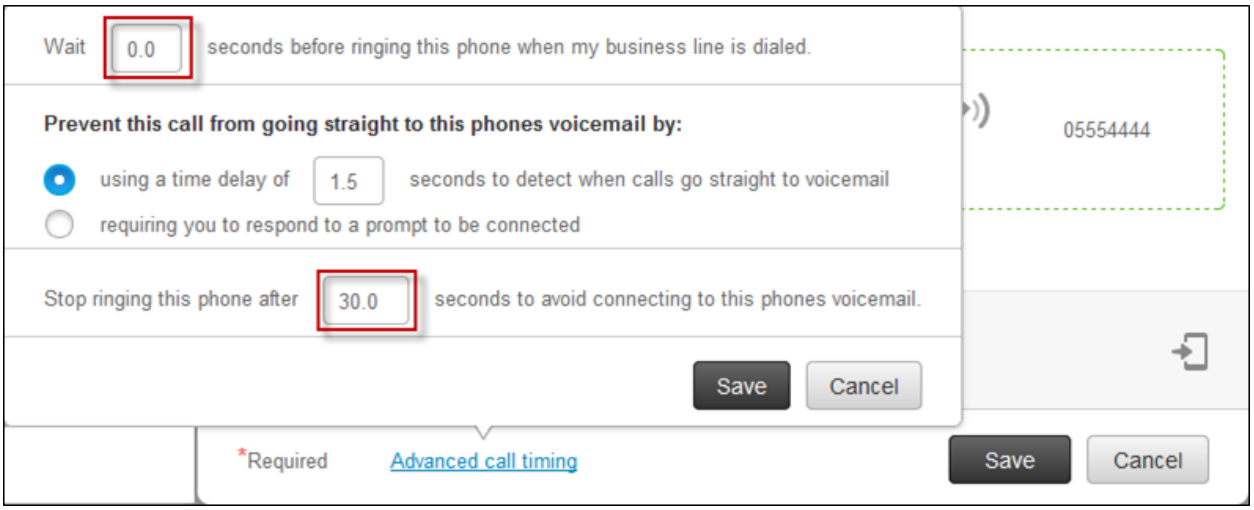
Complete these steps:

Step 37

Navigate to **https://10.1.5.15/ucmuser** and log in with the credentials of **jdoe/cicdpass1!**.

Step 38

Choose the previously configured remote destination of **rd_jdoe** and edit the remote destination. Then click **Advanced call timing** and configure the timers.



Step 39

Save the changes.

Step 40

Place a call from HQ Phone 2 to directory number 2001. The remote destination should ring now within one second. The remote destination should ring for the specified time of 30 seconds.

Activity Verification

You have completed this task when you attain this result:

Both ringer timers have been modified and the results are as configured.

LAB 8: Implement End Users and Voice Mailboxes

LAB8: Implement End Users and Voice Mailboxes

Upon completing this guided lab, you will be able to:

Unlist a user from Cisco Unity Connection

Import end users from Cisco Unified Communications Manager

Import end users from Microsoft Active Directory

Request to initialize lab has been sent

Import End Users from Cisco Unified Communications Manager

In this task, you will import a user, Michael Weston (2003), from Cisco Unified Communications Manager. You will leave and retrieve a message to test the import.

Complete these steps:

Step 1

Open a session to PC1 and login to Cisco Unified Communication Manager Administration (**https://10.1.5.15**) using the browser on the desktop. If you are using Firefox, you will need to add the security exception.

Step 2

Use the appllication user credentials to login to Cisco Unified Communication Manager Administration (**admin** / **cicdpass1!**). Select the **Login** button to continue.

Step 3

In Cisco Unified Communications Manager Administration, select **Device > Phone** and configure the phone button template of **Standard 7965 SCCP** for **HQ Phone 1**. Click **Save** and then click **OK** in the pop-up window. (You may need to reset the phone for the configuration to update).

Step 4

For **HQ Phone 1**, add a second line by selecting **Line 2**. Then, configure the following options:

Second Directory Number: **2003**

Route Partition: **devices**

Calling Search Space: **internal**

Enable Forward Busy for internal and external calls to voicemail

Enable Forward No Answer for internal and external calls to voicemail

Save

Step 5

Navigate to **HQ Phone 2** and configure a phone button template of **Standard 7965 SCCP**. Click **Save** and then click **OK** in the pop-up window.

Step 6

On the phone, to add a second line, click **Line 2** and configure the following:

Second Directory Number: **2004**

Route Partition: **devices**

Calling Search Space: **internal**

Enable Forward Busy for internal and external calls to voicemail

Enable Forward No Answer for internal and external calls to voicemail

Step 7

Open a Remote Desktop connection to the LDAP server at 10.1.5.14, which is a Windows Domain Controller.

Step 8

On the LDAP server, create a new user using the following values and save the configuration:

First Name: **Michael**

Last Name: **Weston**

User Logon Name: **mweston**

Password: **cicdpass1!**

User must change password at next logon: unchecked

Step 9

Perform a complete synchronization of Cisco Unified Communications Manager with the LDAP directory.

Step 10

In Cisco Unified Communications Manager, navigate to **User Management > End Users** and choose **mweston**. Verify the following settings and set the PIN:

User ID: **mweston**

PIN: **131213**

Last Name: **Weston**

First Name: **Michael**

Step 11

To ensure that the Cisco AXL Web Service is activated on Cisco Unified Communications Manager, from the Cisco Unified Communications Manager Serviceability, navigate to **Tools > Service Activation**. Verify that the service is activated, and if not, activate it here.

Step 12

In Cisco Unity Connection Administration, navigate to **Telephony Integrations > Phone System** and choose **CUCM**.

Step 13

Navigate to **Edit > Cisco Unified Communications Manager AXL Servers**.

Step 14

Configure the following settings:

AXL Username: **admin**

Password: **cicdpass1!**

Cisco Unified Communications Manager Version: **5.0 or Greater**

Step 15

Save the configuration.

Step 16

Click **Add New** to add a new AXL server. Enter the following configuration:

IP Address of Cisco Unified Communications Manager: **10.1.5.15**

Port: **8443**

Step 17

Save the configuration.

Step 18

After saving the configuration, click the **Test** button to test the AXL connection. The message “Test message successfully sent to AXL server 10.1.5.15:8443.” should appear.

Step 19

Navigate to **Users > Import Users**. In the Find End User In drop-down list, choose **CUCM** and then click **Find**. You will see Jane White and John Doe.

Note: An end user in Cisco Unified Communications Manager must have a primary extension that is configured to be imported.

Step 20

Choose both users and click the **Import Selected** button. In the pop-up window that appears, notice that there is an import failure. Click the log file link and view the reasons for the failure.

Step 21

In Cisco Unified Communications Manager Administration, go to the user **mweston**, click **Device Association**, and then click **Find**.

Step 22

Choose the device with the directory number **2003** and click **Save Selected/Changes**. In the Related Links box, choose **Back To User** and click **Go**.

Step 23

In the user configuration, set the Primary Extension to **2003 in devices** and save the configuration.

Step 24

In Cisco Unity Connection Administration, navigate to **Users > Import Users**. In the Find End User In drop-down list, choose **CUCM** and then click **Find**. The user mweston should now appear.

Step 25

From the Based-on Template drop-down list, choose **CICD User Template**. Check the check box for **mweston** and click **Import Selected**.

Step 26

A status message appears: “Importing users completed. Number of successes: 1, Number of failures: 0.” If you do not see any successes, verify you completed the previous steps.

Step 27

Navigate to **Users > Users** and choose **mweston**. Uncheck the **Set for Self-enrollment at Next Sign-In** check box and save the configuration. Navigate to **Edit > Password Settings** and uncheck the **User Must Change at Next Sign-In** check box. Navigate to **Edit > Change Password** and set the PIN to 131213.

Note

This user is integrated from Cisco Unified Communications Manager. Some fields in the user configuration can be disabled.

Activity Verification

You have completed this task when you attain these results:

Verify that mweston has been imported from Cisco Unified Communications Manager into Unity Connection.

Note: When logging in, notice that the PIN is not imported from Cisco Unified Communications Manager. The password is also not imported from Cisco Unified Communications Manager.

Import End Users from Microsoft Active Directory

In this task, you will import the user Arvin Sloane (2004) from an LDAP server. You will leave and retrieve a message to test the configuration.

Complete these steps:

Step 28

Open a Remote Desktop connection to the LDAP server at 10.1.5.14.

Step 29

On the LDAP server, create a new user, using the following values, and save the configuration:

First Name: **Arvin**

Last Name: **Sloane**

User Logon Name: **asloane**

Password: **cicdpass1!**

User must change password at next logon: Unchecked

Step 30

Right-click the new user and choose **Properties**.

Step 31

In the Telephone Number field, enter **2004** and click **OK**.

Step 32

In Cisco Unified Serviceability of Cisco Unity Connection, navigate to **Tools > Service Activation**. Activate the **Cisco DirSync** service.

Step 33

In Cisco Unity Connection Administration, navigate to **System Settings > LDAP > LDAP Setup**.

Step 34

Set the following parameters and save the configuration:

Enable Synchronizing from LDAP Server: Checked

LDAP Server Type: **Microsoft Active Directory**

LDAP Attribute for User ID: **sAMAccountName**

Step 35

Navigate to **System Settings > LDAP > LDAP Directory Configuration**. Click **Add New**, configure the following parameters, and save the configuration:

LDAP Configuration Name: **LDAP Server**

LDAP Manager Distinguished Name: **administrator@ciscoclass.com**

LDAP Password: **cicdpass1!**

LDAP User Search Base: **dc=ciscoclass, dc=com**

Perform Sync Just Once: Checked

LDAP hostname or IP Address: **10.1.5.14**

Note: In the lab, the Microsoft Administrator account (full access rights) is used. In non-lab environments, the Microsoft Domain Administrator will provide you with an account that will have the relevant access rights.

Step 36

Click **Perform Full Sync Now** (located at the bottom of the page).

Note

Even if only four users are configured on the LDAP server, the first synchronization can take up to 5 minutes. The following synchronizations are done in seconds.

Step 37

Navigate to **Users > Import Users**. From the Find End Users In drop-down list, choose **LDAP Directory**.

Step 38

Click **Find**. The previously configured user, Arvin Sloane, should appear. Additional users may appear.

Note

If an LDAP synchronization is not performed, no users are shown. If, for example, the LDAP User Search Base is incorrect, users will not be shown.

Step 39

From the Based-on Template drop-down list, choose **CICD User Template**. Check the check box for **asloane** and click **Import Selected**.

Step 40

The import should be successful and display the message states: “Importing users completed. Number of successes: 1, Number of failures: 0.” If you do not see any successes, verify you completed the previous steps.

Step 41

Select **System Settings > Authentication Rules**. Then, choose the Recommended Voice Mail Authentication Rule and change the **Minimum Credential Length** to **3**. Select **Save**.

Step 42

From the Users page, choose **asloane**. Compared to the Cisco Unified Communications Manager imported user, the extension field for asloane is not a read-only field. Uncheck the **Set for Self-enrollment at Next Sign-In** check box and save the configuration. Navigate to **Edit > Password Settings** and uncheck the **User Must Change at Next Sign-In** check box. Navigate to **Edit > Change Password** and set the PIN to 321.

Step 43

In preparation for the Cisco Jabber lab, enable Web login authentication via LDAP: Navigate to **System Settings > LDAP > LDAP Authentication**, configure the following and save the configuration:

Use LDAP Authentication for End Users: checked

LDAP Manager Distinguished Name: **administrator@ciscoclass.com**

LDAP Password: **cicdpass1!**

LDAP User Search Base: **dc=ciscoclass, dc=com**

LDAP hostname or IP Address: **10.1.5.14**

Activity Verification

You have completed this task when you attain these results:

Verify that asloane has been imported from LDAP into Unity Connection

LAB9: Enable Cisco Unified Communications Manager IM and Presence Service

LAB9: Enable Cisco Unified Communications Manager IM and Presence Service

Upon completing this guided lab, you will be able to:

Configure Cisco Unified Communications Manager for Cisco Jabber

Create a CSF Device for Softphone Mode

Configure the Cisco Unified IM and Presence Server to support Cisco Jabber

Log in and test Cisco Jabber

Use Cisco Jabber in softphone and deskphone mode

Request to initialize lab has been sent

Configure Cisco Unified Communications Manager for Cisco Jabber

For Cisco Jabber usage, configure end users in Cisco Unified Communications Manager. Assign the IM and Presence capabilities to jdoe and jwhite along with a Service Profile. Configure line association for the directory numbers 2001 and 2002. Then, enable both end users for CTI control and associate the device.

Complete these steps:

Configure End Users in Cisco Unified Communications Manager

In this section, you will configure jdoe and jwhite in Cisco Unified Communications Manager for Cisco Jabber usage:

Step 1

Navigate to **Device > Phone** and choose **HQ Phone 1**. Choose directory number **2001**.

Step 2

At the bottom of the page, verify that jdoe is associated with the directory number. If not, click **Associate End Users** and then click **Add Selected** to add a user with the User ID jdoe. Save the changes and click **Apply Config**. This is required to subscribe to the current line state in Cisco Jabber.

Step 3

Repeat Step 2 for jwhite and HQ Phone 2 with the directory number 2002.

Step 4

Navigate to **User Management > User Settings > UC Service** and view the UC Services that have been configured prior to the start of class:

CTI: Points to the Cisco Unified Communications Manager

Mailstore: Points to the Cisco Unity Connection and enables Visual Voicemail

Voicemail: Points to the Cisco Unity Connection for playing voicemails

IM and Presence: Defines which IM And Presence server to obtain presence information from

Directory: Defines the LDAP directory used to look up users

Assign the IM and Presence Capabilities and Configure Line Association

In this section, you will assign the IM and Presence capabilities to jdoe and jwhite along with a Service Profile, and configure line association for the directory numbers 2001 and 2002:

Step 5

Navigate to **User Management > User Settings > Service Profile** and click **Find**. Choose the Service Profile named **Jabber_SP** that was configured prior to the start of class. Note that the UC Services that are applied to the Jabber_SP Service Profile are the UC Services that were viewed in the previous task. In the Directory Profile section, change the Username to: **administrator@ciscoclass.com** and click **Save**.

Step 6

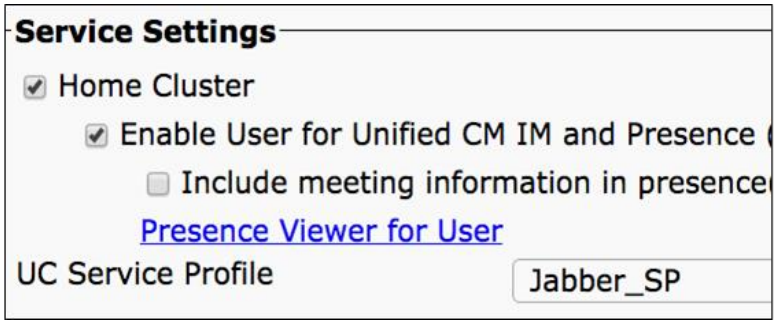
Navigate to **User Management > End User** and search for user **John Doe**.

Step 7

Under Service Settings, verify the following settings:

Enable User for Unified CM IM and Presence: **checked**

UC Service: **Jabber_SP**



Step 8

To enable desk phone control, click **Device Association** and then **Find**. The user must be associated with the device that has directory number 2001. Go back to the user configuration page.

Note

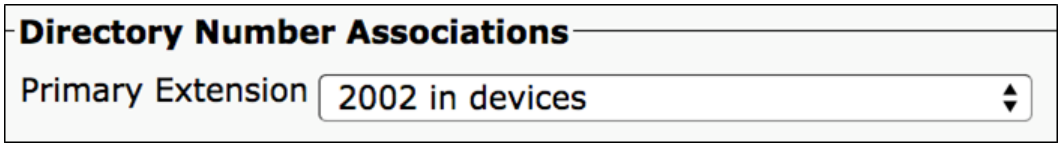
This association is per device. Therefore, all or no lines of the same device are selected.

Step 9

Click **Line Appearance Association for Presence** and then verify that the line of HQ Phone 1 with directory number 2001 is checked. Go back to the user configuration page.

Step 10

Ensure that the Primary Extension is set to 2001 in devices for jdoe.



Step 11

Repeat Steps 6–11 for jwhite with the following differences: the associated device is HQ Phone 2, the line appearance association for presence is 2002, and the primary extension is 2002 in devices.

Enable Users for CTI Control and Associate the Device

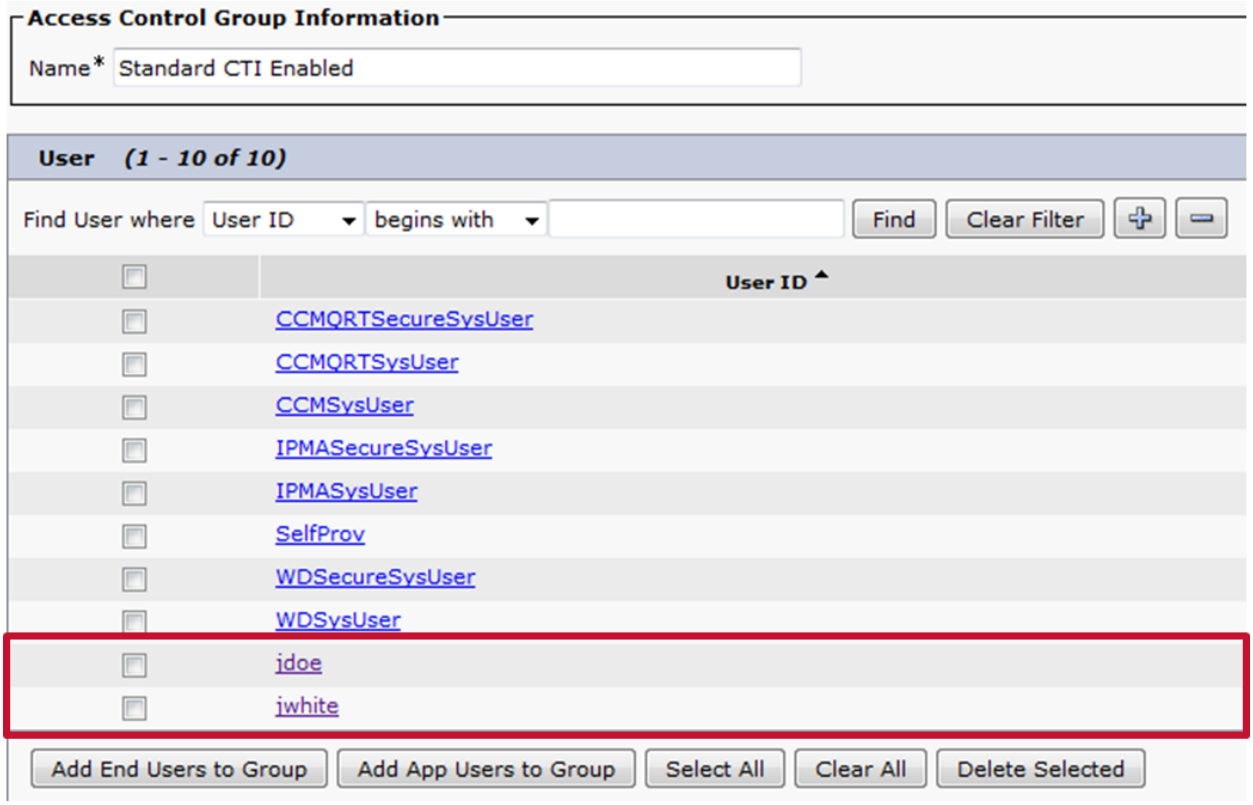
In this section you will enable both end users for CTI control and associate the device.

Step 12

To enable CTI control, you must add the end user to the correct user group. Navigate to **User Management > User Settings > Access Control Group**.

Step 13

Click the **Standard CTI Enabled** group and then click **Find** to list the members of the group. User jdoe and jwhite need to be members of the group. Use the **Add End Users to Group** button to add end users to the group, if needed.



Step 14

In the Related Links field, select **Back to Find/List** and click **Go**.

Step 15

To enable end-user login on the Cisco Unified Communications Manager IM and Presence Service end-user web pages, verify the Group assignment and, if not configured, add both users to the Standard CCM End Users group.

Step 16

In the Related Links field, select **Back to Find/List** and click **Go**.

Step 17

Because you are using the Cisco Unified IP Phone 9900 Series model phones in the lab, you have to add users jdoe and jwhite to the **Standard CTI Allow Control of Phones Supporting Connected xfer and Conf** group. Verify that the **Standard CCM Users - Standard CTI Allow Control of phones supporting** and **Standard CTI Enabled** are in the group assignments for both users **jdoe** and **jwhite**.

Note

The Cisco Unified IP Phones 6900 and 8900 Series phones still require the Standard CTI Enabled and Standard CCM End Users groups.

Step 18

Navigate to **Device > Phone** and choose the HQ Phone 1 endpoint.

Step 19

Choose the line **2001** on the left side of the page to enter the line configuration page.

Step 20

For line 2001, verify that the **Allow Control of Device from CTI** check box is checked. This allows the Cisco Jabber software to control the physical endpoint using CTI when operating in desktop mode.

Step 21

Navigate to **Device > Phone** and choose the HQ Phone 2 endpoint.

Step 22

Choose the line **2002** on the left side of the page to enter the line configuration page.

Step 23

For line 2002, verify that the **Allow Control of Device from CTI** check box is checked. This allows the Cisco Jabber software to control the physical endpoint using CTI when operating in desktop mode.

Activity Verification

You have completed this task when you attain this result:

The configuration will be tested in the next tasks.

Create a CSF Device for Softphone Mode

Create a softphone for user John Doe. Configure a new Cisco Unified CSF device in Cisco Unified Communications Manager and configure the line association. Then, associate the end user with the Cisco Unified CSF device.

Complete these steps:

Step 24

Navigate to **Device > Phone** and add a new device.

Step 25

Choose **Cisco Unified Client Service Framework** as the device type and click **Next**.

Step 26

Use the following values to create the Cisco CSF device:

Device Name: **CSFJDOE**

Description: **Jabber Softphone for jdoe**

Device Pool: **Default**

Phone Button Template: **Standard Client Service Framework**

Calling Search Space: **pstn**

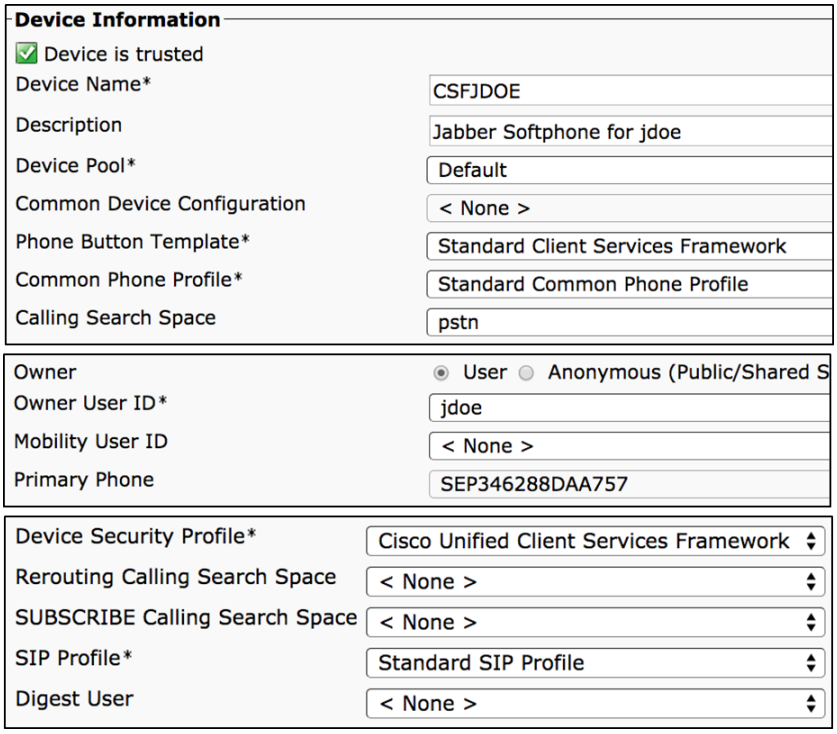
Owner User ID: **jdoe**

Primary Phone: Use the Device Name of HQ Phone 1 (SEP111111111111)

Note: When a primary phone is selected, Cisco Unified Communications Manager uses adjunct licensing for Cisco Unified CSF clients.

Device Security Profile: Cisco Unified Client Service Framework – Standard SIP Non-Secure Profile

SIP Profile: Standard SIP Profile



Step 27

Save the changes.

Step 28

Now to add the directory number 2001 to the device, click **Line [1] – Add a new DN**.

Step 29

Configure the directory number 2001 and choose **devices** as the route partition. Click into another field to reload the page. **Save** the changes.

Step 30

At the bottom of the page, click **Associate End Users** and associate end user jdoe with the line.

Step 31

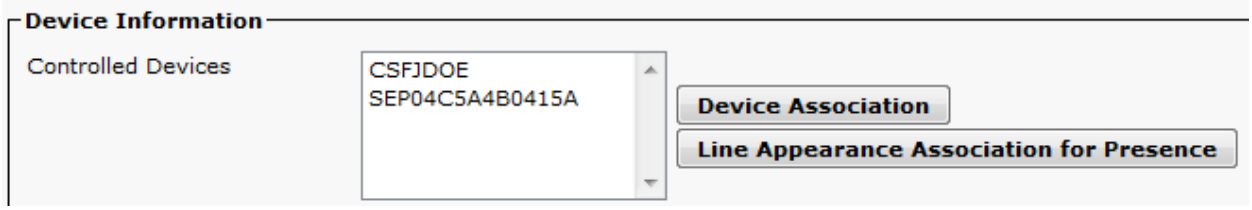
Save the changes and apply the configuration.

Step 32

Navigate to **User Management > End User** and search for the user ID jdoe. Click **Device Association** and search the newly created CSF device. Associate the device and save the changes.

Step 33

From Related Links, choose **Back to User** and click **Go**. Verify that the associated CSF device (CSFJDOE) is listed in the Controlled Devices box.



Step 34

Repeat Steps 1 through 10 for jwhite and DN 2002.

Activity Verification

You have completed this task when you attain this result:

The configuration will be tested in the next tasks.

Configure the Cisco Unified IM and Presence Server

To configure Cisco Unified IM and Presence server to support Cisco Jabber, a SIP Publish trunk and a SIP Presence Gateway must be set.

Step 35

Open the Cisco Unified IM and Presence administrator web interface in the web browser (**https://10.1.5.18/cupadmin**).

Step 36

Navigate to **Presence > Settings > Standard Configuration** and, from the CUCM IM and Presence Publish Trunk drop-down list, choose **IMP_Trunk**, which is a SIP trunk that was predefined on the Cisco Unified Communications Manager. Click **Save**.

Step 37

Navigate to **Presence > Gateways** and configure the presence gateway with the following configuration:

Presence Gateway Type: **CUCM**

Description: **Cisco Unified Communications Manager**

Presence Gateway: **10.1.5.15**

Step 38

Navigate to **Cisco Unified IM and Presence Servicability**.

Step 39

Navigate to **Tools > Service Activation**.

Step 40

From the Server drop-down menu, choose **10.1.5.18—CUCM IM and Presence**.

Step 41

Verify that the check boxes for the following services are checked, or check them if necessary:

Cisco XCP Directory Service

Cisco AXL Web Service

Cisco SIP Proxy

Cisco Presence Engine

Cisco XCP Text Conference Manager

Cisco XCP Connection Manager

Cisco XCP Authentication Service

Step 42

Click **Save** and **OK** in the pop-up window.

Activity Verification

You have completed this task when you attain this result:

The SIP Publish trunk and a SIP Presence Gateway are set.

Log in to Cisco Jabber

Cisco Jabber is pre-installed on the Student PCs. Use the values that are shown in the following table:

Parameters		
Computer	Username	Password
PC 1	N/A	cicdpass1!
Phones PC	N/A	cicdpass1!

Step 43

Start Cisco Jabber from the Student PC 1(jdoe).

Step 44

Click the **Settings** button on the top right corner of the Cisco Jabber application window and choose **File > Reset Cisco Jabber** to erase any configuration settings that may exist from previous use. If the option is greyed out, then there are no stored settings.

Step 45

Enter **jdoe@ciscoclass.com** and click **Continue**. Cisco Jabber detects your services via DNS and when done you are prompted to enter your username and password for phone services. Enter **jdoe** and **cicdpass1!** and click **Sign In**.

Step 46

Should you get a “Username or Password is incorrect” message, navigate to the device DC-HQ. Click on the **Start** button and select “**Active Directory Computers and Users**”. Locate user John Doe. Right click

on the user and select “**Reset Password**”. Change the password to: **cicdpass1!** and click **OK**. Repeat the process for user Jane White.

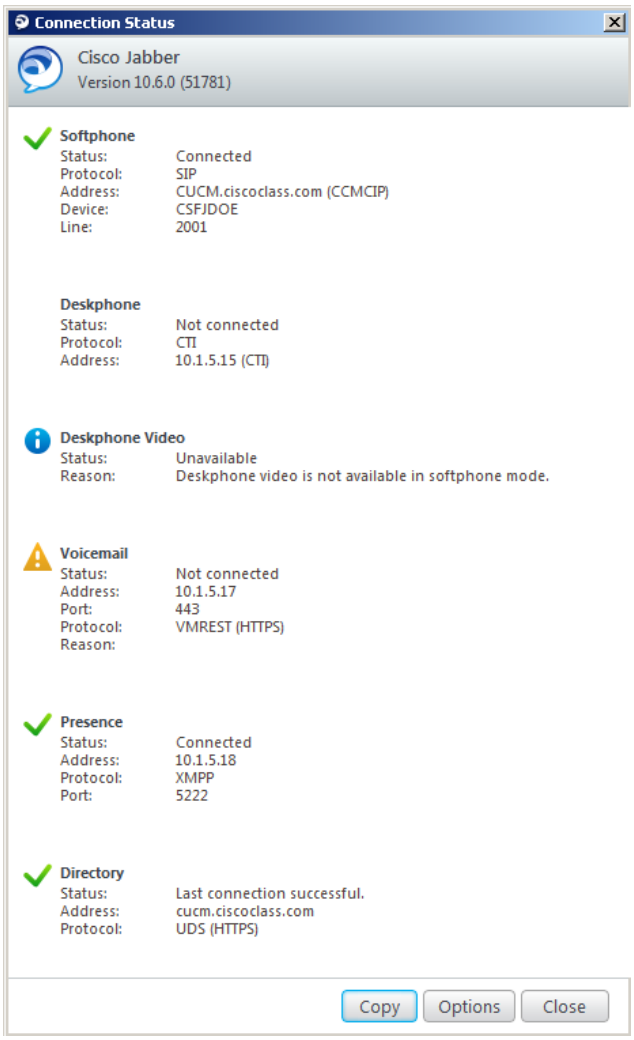
Note:If prompted to trust any certificates, click Accept.

Step 47

Click **Cancel** if there is a pop window that reports a location update.

Step 48

In Cisco Jabber, navigate to **Help > Show Connection Status**.



Note:When Cisco Jabber is in softphone mode, there is no status for hard phone mode and vice versa. Voicemail is not connected because you would have to set the Voicemail credentials. You can do this by clicking the Options button at the

Connection Status window. However, the end users in Cisco Unity Connection have not been configured with a Web Application password. In this lab, this is not required, because you are not using voicemail on Cisco Jabber.

Step 49

Repeat the previous steps on Phones PC for user jwhite.

Note

If the Directory is not showing connected, you may need to restart the Cisco Unified IM & Presence server. Using putty (on the pc desktop), ssh to 10.1.5.18, with the admin credentials and issue the command **utils system restart**. You will need to wait about 10 minute for all services on the server to stabilize.

Activity Verification

You have completed this task when you attain these results:

You successfully logged in to Cisco Jabber.

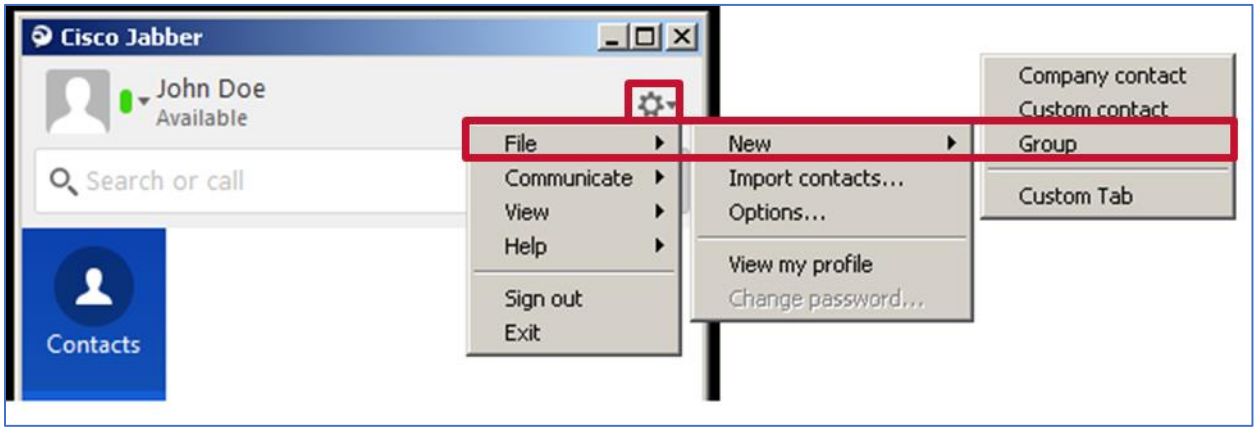
The Softphone, Presence, and Directory services are shown as "Connected."

Test Cisco Jabber Features

Add the users as contacts on Cisco Jabber. Use the Cisco Jabber client of jdoe in softphone mode. Test CTI control with the Cisco Jabber Communicator of jwhite.

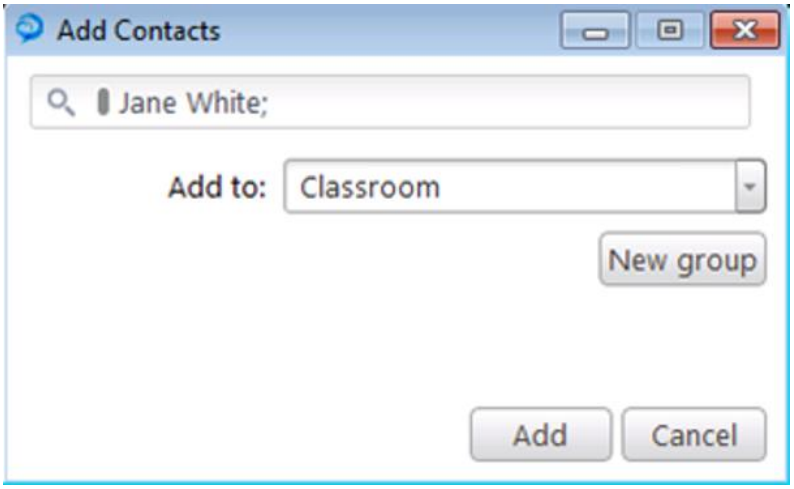
Step 50

On Student PC 1 (Cisco Jabber), navigate to **File > New > Group**. In the pop-up window, enter a Group Name of **Classroom**.



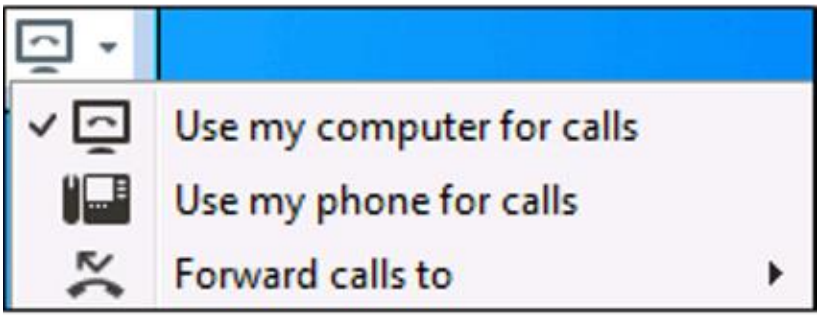
Step 51

On Student PC 1 (Cisco Jabber), navigate to **File > New > Company Contact**. In the Search field, enter **Jane White** and in the Add To drop-down list, choose the **Classroom** group and click **Add**.



Step 52

On Student PC 1, use the icon in the lower left corner of the Cisco Jabber window to verify that Cisco Jabber is in softphone mode (Use my computer for calls).

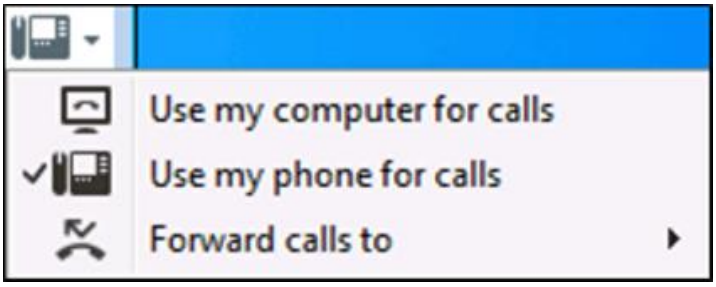


Step 53

On Phones PC (Cisco Jabber), navigate to **File > New > Company Contact**. In the Search field enter **John Doe** and add this user to the Classroom group of Jane White. You can create the group by clicking **New group** in the Add Contacts window.

Step 54

On Student PC 2, click the icon in the lower-left corner of the Cisco Jabber window and choose **Use my phone for calls** to put Cisco Jabber into deskphone mode. Make sure that your HQ Phone instances are started up. Once you set Jabber in deskphone mode, you may see errors on the phone display. Click **Exit** on the phone button.



Step 55

Place a call with the Cisco Jabber of jdoe (2001) to jwhite (2002). Answer the call with the Cisco Jabber of jwhite to test CTI control.

Step 56

Place a call from the phone of jwhite (2002) to jdoe (2001) and notice that the call is sent to the desk phone (2001) and to Cisco Jabber of user jdoe.

Step 57

From Jabber on Student PC 1, right-click **Jane White**, choose **Chat,** and exchange messages between the Cisco Jabber applications on the two PCs.

Activity Verification

You have completed this task when you attain these results:

You successfully logged in to Cisco Jabber.

You successfully placed and answered a call.

You exchanged chat messages.

You used deskphone and softphone mode

LAB10: Generate Cisco Unified Communications Manager CAR Tool Reports

LAB10: Generate Cisco Unified Communications Manager CAR Tool Reports

Request to initialize lab has been sent

Analyze Calls

Complete the following:

Step 1

Use the Cisco Unified Communications Manager CAR tool to analyze the latest placed call from HQ Phone 1 (directory number 2001) to HQ Phone 2 (directory number 2002). Obtain values for partition, jitter, latency, and IP addresses, and note them in the table.

Parameter	Value
Partition of calling number	
IP address of destination	
Jitter of the calling party	
Latency of the destination	

Activity Verification

You have completed this task when you attain these results:

The partition, jitter, latency, and IP addresses of the call from HQ Phone 1 (directory number 2001) to HQ Phone 2 (directory number 2002) is determined.

The CDR search generates a report showing the recently placed calls

LAB11: Monitor the System with Cisco Unified RTMT

LAB11: Monitor the System with Cisco Unified RTMT

Upon completing this guided lab, you will be able to:

Install the Cisco Unified RTMT tool

Monitor the system and server capacity

Use traces and syslog messages

Monitor the Cisco Unified Communications Manager, call and trunk activity, device summary, and Cisco TFTP

Create and use profiles

Use the port monitor to check the voicemail ports

Request to initialize lab has been sent

Log in to Cisco Unified RTMT

In this task, you will log into the Cisco Unified RTMT and connect to the Cisco Unified Communications Manager.

Complete these steps:

Step 1

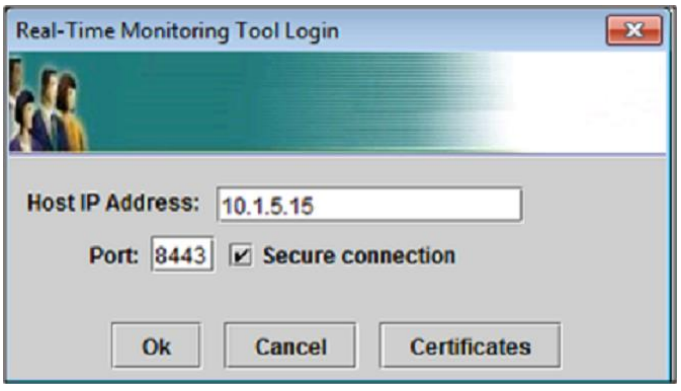
Start the Cisco Unified RTMT.

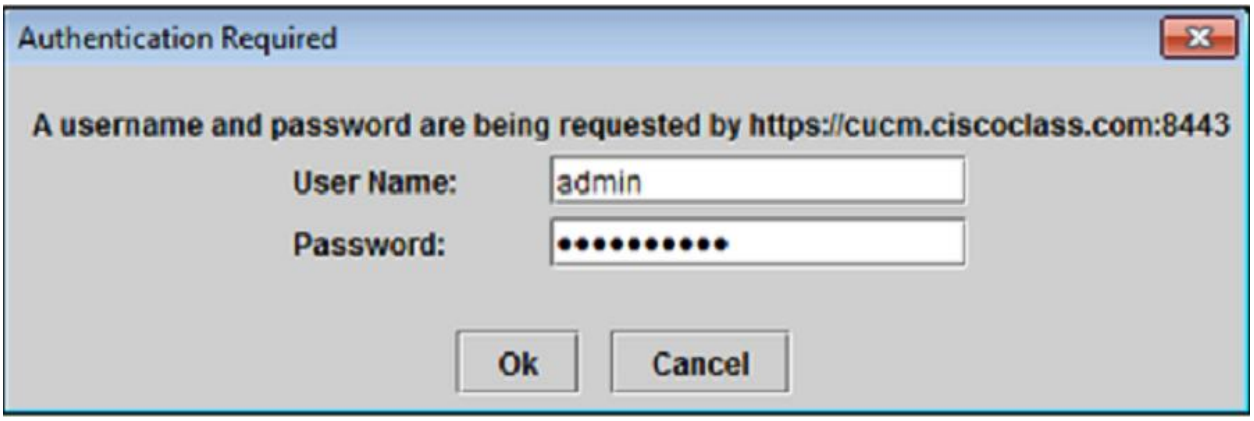
Step 2

Cisco Unified RTMT establishes a secure connection to Cisco Unified Communications Manager. It is necessary to add the certificate to the local trust store. Click **Accept**.

Step 3

Enter **10.1.5.15** for the IP address of the Cisco Unified Communications Manager. Enter the application user of username **admin** and password **cicdpass1!** to log in.





Step 4

When Cisco Unified RTMT is open, click **Cancel** in the Select Configuration window to start a new, blank monitoring pane.

Activity Verification

You have completed this task when you attain this result:

Can successfully log in to Cisco Unified Communications Manager with RTMT.

Monitor System Parameters

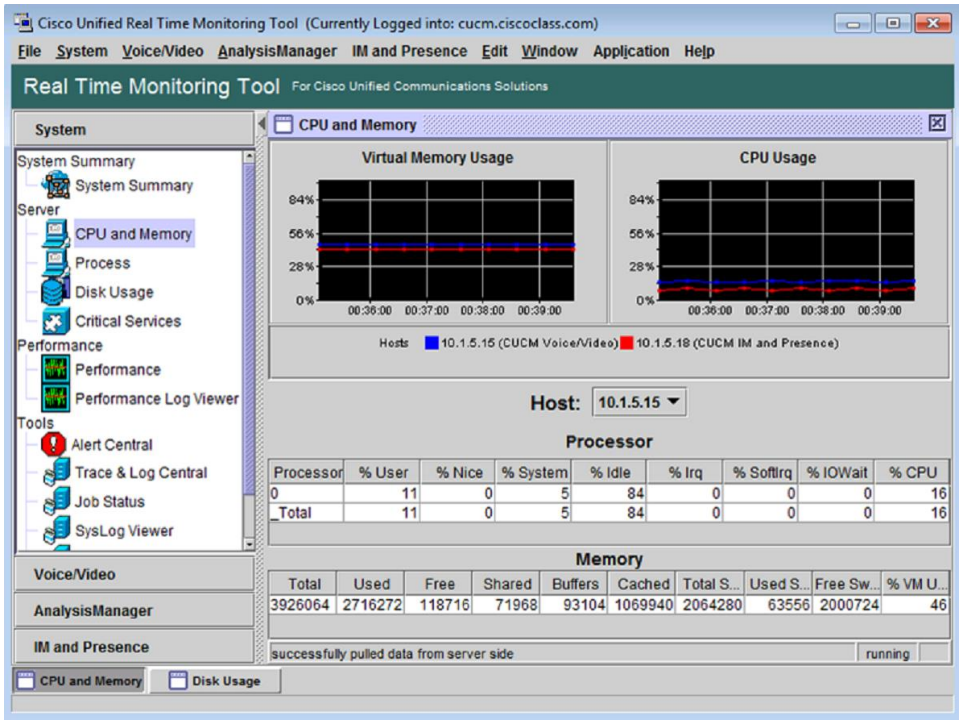
In this task, you will use the System submenu to monitor system parameters. Explore different categories in the System submenu to fill out the following table with the system values. Then enable sending alerts by email to admin@cisco.com using mail.cisco.com as the email server. Set the threshold for the call processing node to 95 percent in the alert central.

System Parameter	Value
Virtual Memory used (%)	
Common Partition Usage (%)	
Tx Errors on Network Interface Eth0	
Rx Errors on Network Interface Eth0	

Complete these steps:

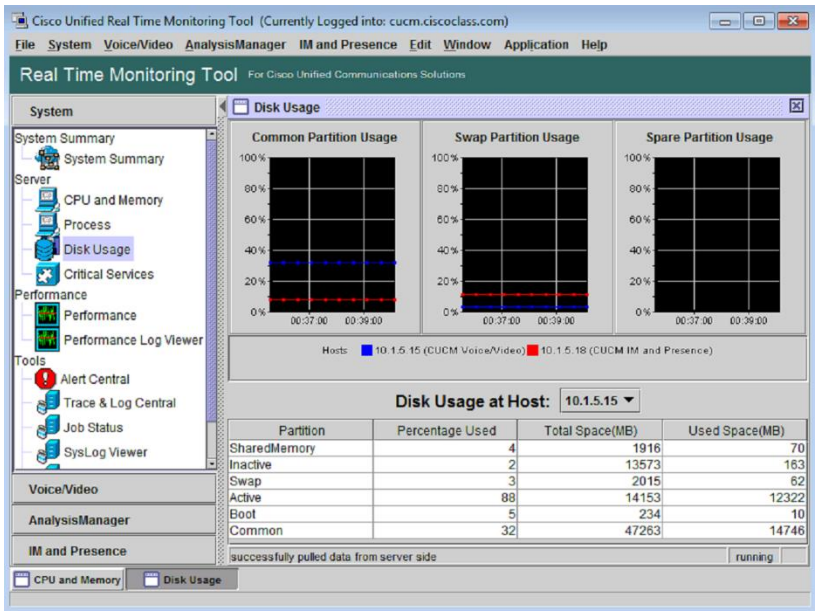
Step 5

In Cisco Unified RTMT, choose **System > Server > CPU and Memory**. Obtain the % VM Used value from the Memory table and note it in the table at the beginning of this task. You will need to wait a few minutes for the graphics to start populating with the data.



Step 6

Open the **Disk Usage** category. Note the percentage usage of the Common partition in the table.



Step 7

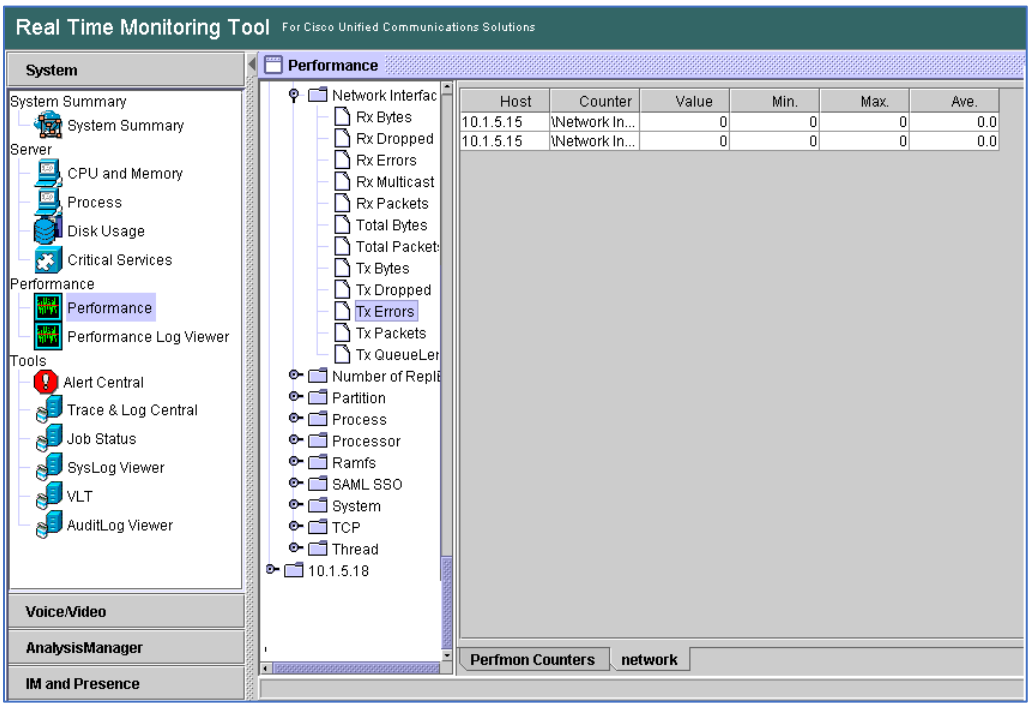
Open the **Performance** category. In the bottom toolbar, right-click **Perfmon Counters** and choose **New Category**. Use network as the new name and check the **Present Data in Table View** check box.

Step 8

In the Performance category tree, navigate to **Network Interface > Rx Errors** and use drag and drop to add this value to the table. For the Object Instant value, choose **eth0** and click **Add**.

Step 9

Repeat the previous step with the Tx Errors counter and note both values in the table.



Step 10

Navigate to **System > Tools > Alert > Config Email Server**.

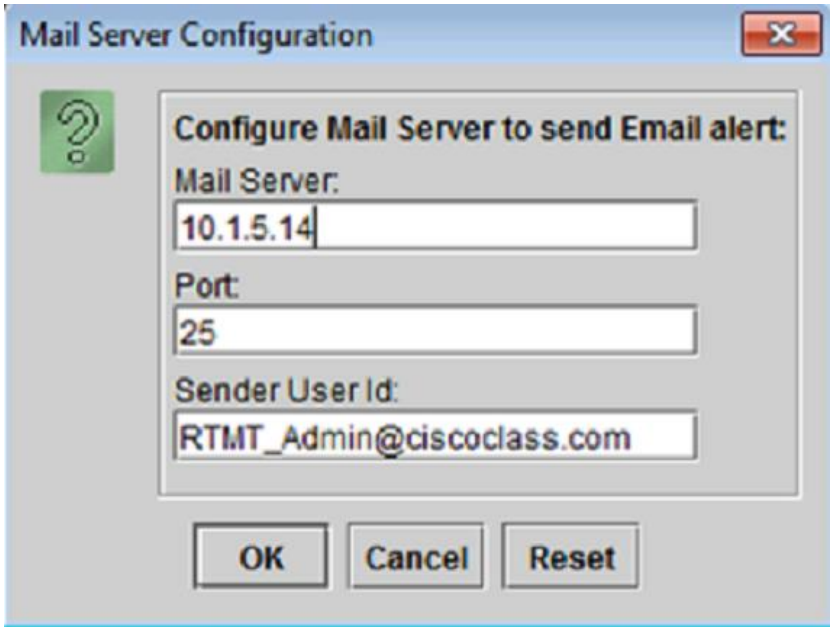
Step 11

Enter the following values in the window that appears:

Mail Server: **10.1.5.17**

Port: **25**

Sender User ID: **RTMT**

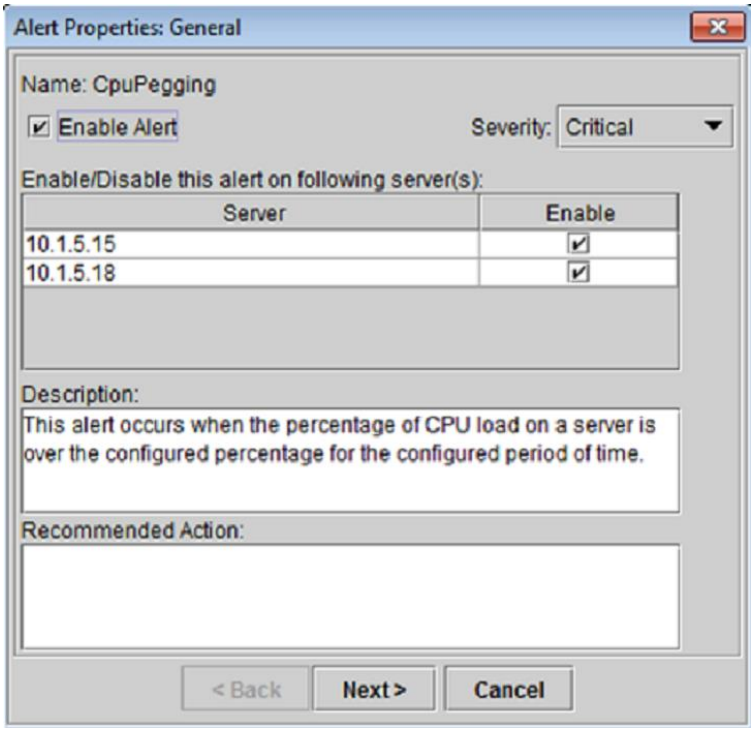


Step 12

To set the alert configuration, navigate to **System > Tools > Alert > Alert Central**.

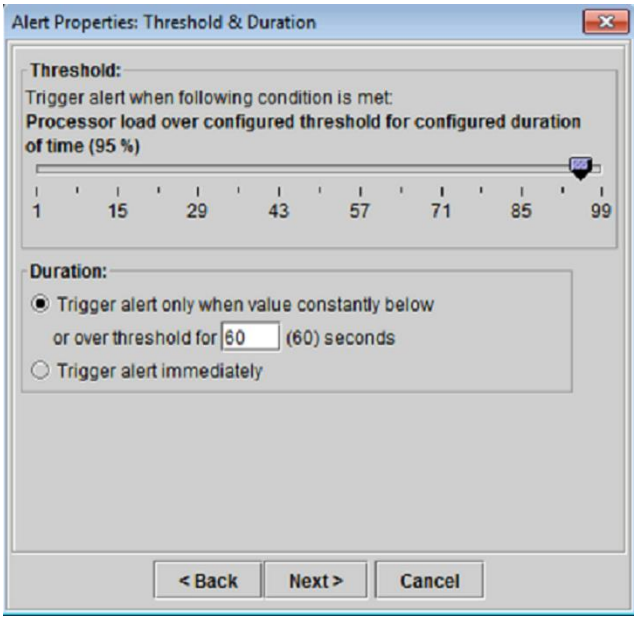
Step 13

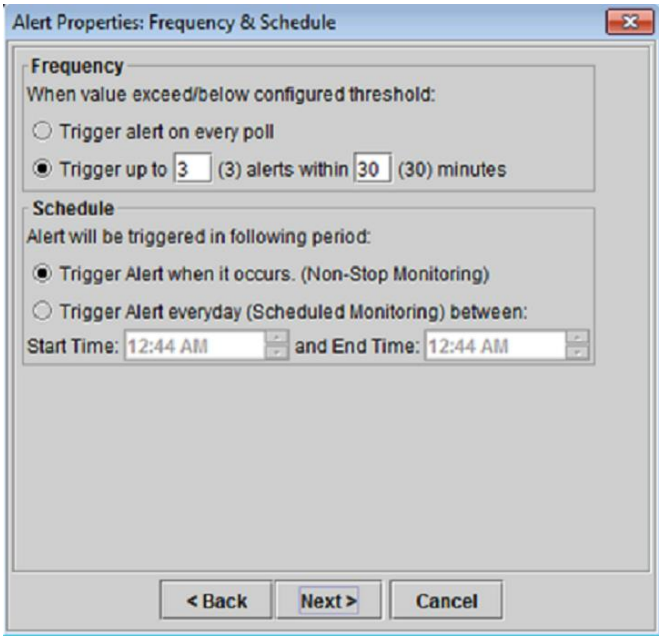
Right-click **CpuPegging** and choose **Set Alert/Properties.**

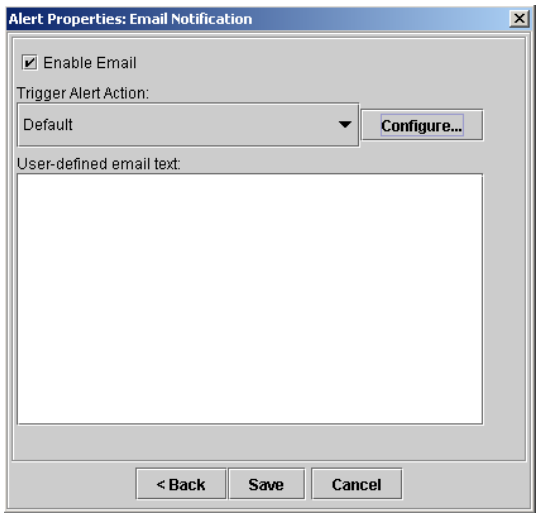


Step 14

Click **Next** to configure the Threshold values. Set the threshold value to **95%**, click **Next**, and click **Next** again.





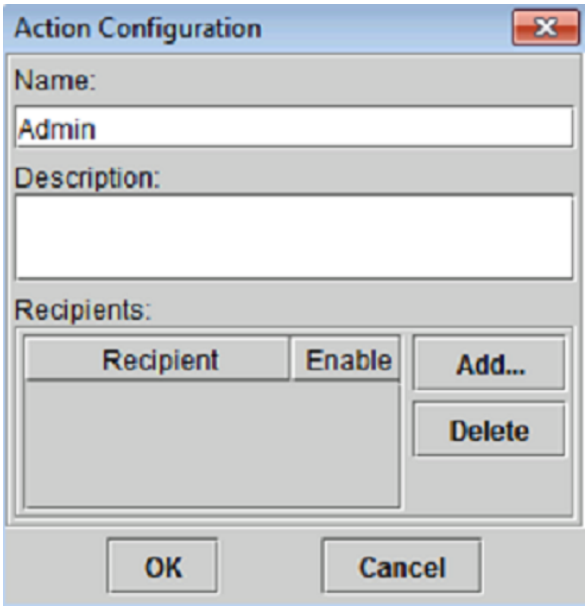


Step 15

Click **Configure** and then click **Add**.

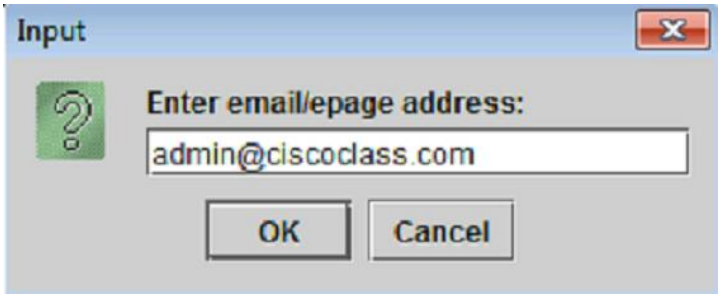
Step 16

Enter a name of **Admin** and then click **Add** at the right of the recipient section.



Step 17

Enter an email address of **admin@ciscoclass.com** and then click **OK**. Click **OK** again when prompted. Then click **Close**.



Step 18

From the Trigger Alert Action drop-down list, choose the alert action **admin**, enter a user-defined email text of **CPU Usage High**, and then save the configuration.

Activity Verification

You have completed this task when you attain these results:

The values requested in the table at the beginning of this task have been discovered.

The alert configuration and threshold have been configured.

Work with Traces and Syslog Messages

In this task, you will use Remote Browse to manually download the latest Cisco CallManager service SDI file and open the syslog messages to display application errors, and download them.

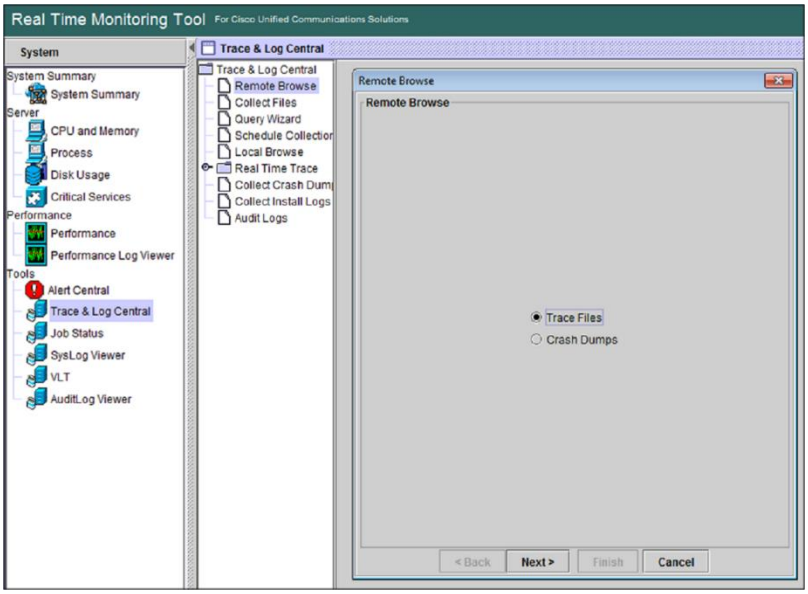
Complete these steps:

Step 19

From the System submenu, choose **Trace & Log Central** and double-click **Remote Browse**.

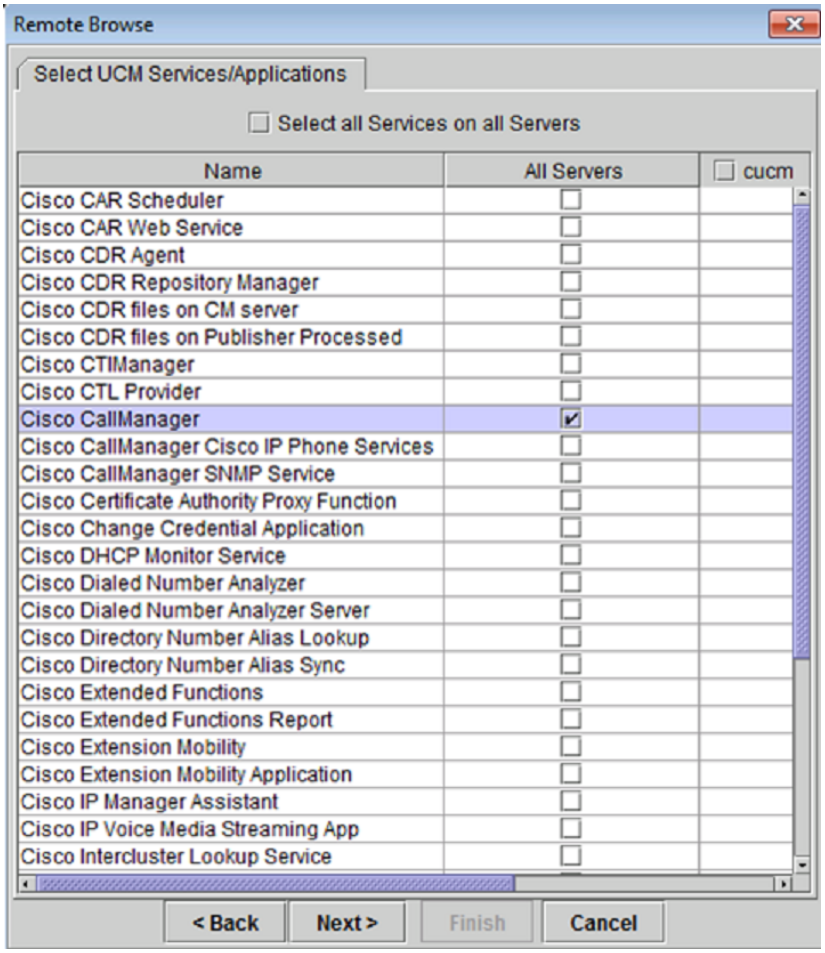
Step 20

Choose **Trace Files** and click **Next**.



Step 21

From the Select UCM Services/Applications tab, check the **Cisco CallManager** check box. You can check Cisco CallManager at the All Servers column because only one server exists.



Step 22

Click **Next**, click **Next** again, and then click **Finish** to start the remote browse.

Step 23

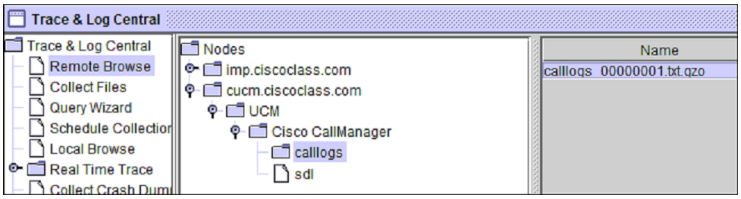
Wait until Cisco Unified RTMT responds with a pop-up message that the remote browse is ready and click **Close**.

Step 24

Navigate to **Nodes > cucm.ciscoclasss.com > UCM > Cisco CallManager** and double-click **calllogs**.

Step 25

Sort the files by the modified date and double-click the latest file.



Step 26

Choose the **Generic Log Viewer** and then click **OK**. View the output and then click **Close**.

Activity Verification

You have completed this task when you attain this result:

You successfully viewed a call log file.

Monitor Cisco Unified Communications Manager Parameters

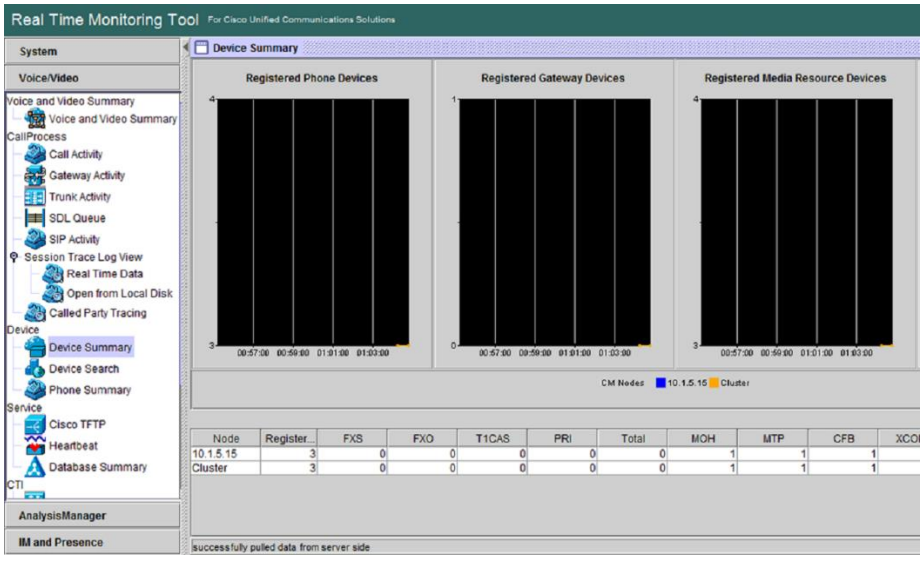
In this task, you will use the Cisco Unified RTMT to monitor Cisco Unified Communications Manager parameters. Then, you will obtain the phone load version of HQ Phone 1 using the Device Search. Note all values in the following table.

Cisco Unified Communications Manager parameter	Value
Current devices registered	
Aborted TFTP requests	
H.323 trunk calls completed	
Phone load of HQ Phone 1	

Complete these steps:

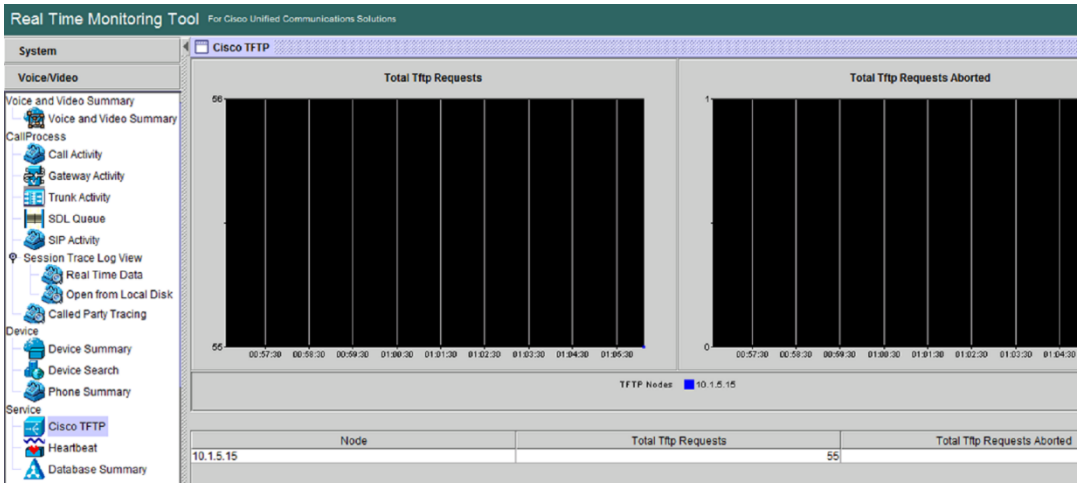
Step 27

Click the **Voice/Video** tab and choose **Device Summary**. Note the Registered Phone Devices value.



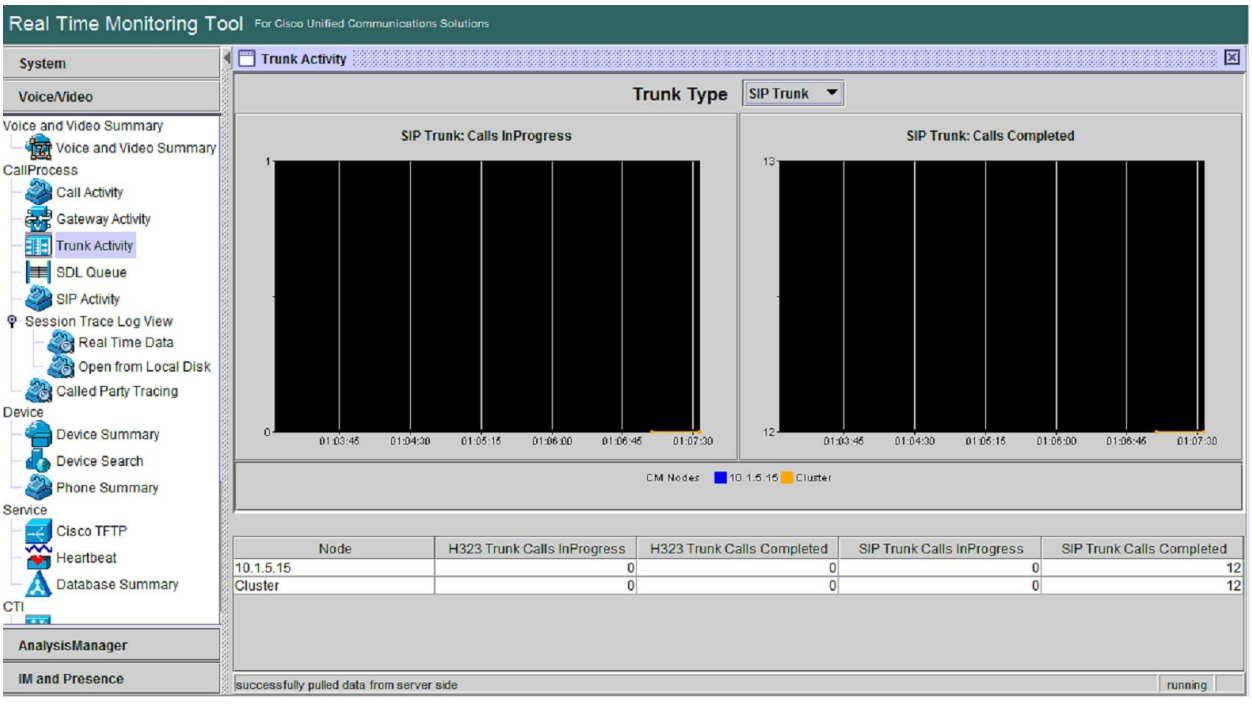
Step 28

To view the TFTP activity of Cisco Unified Communications Manager, choose **Cisco TFTP**. The graph shows the total and aborted TFTP requests. Record the value in the table.



Step 29

Next, open the **Trunk Activity** category. From the Trunk Type drop-down list, choose **SIP Trunk** to monitor the SIP trunks and note the SIP Calls Completed value.

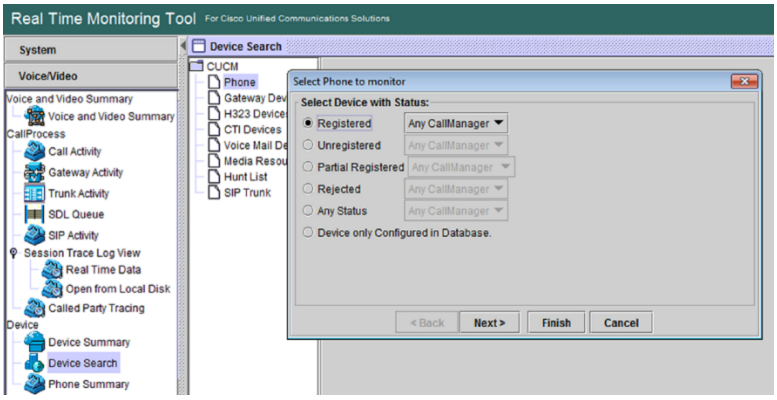


Step 30

The device search allows administrators to run search requests to obtain the status of phones, gateways, hunt lists, and more. From the CallManager submenu, navigate to **Device Search > Phone** to search for IP phones.

Step 31

Search for registered phones, choose **10.1.5.15** from the drop-down list, and then click **Next**.

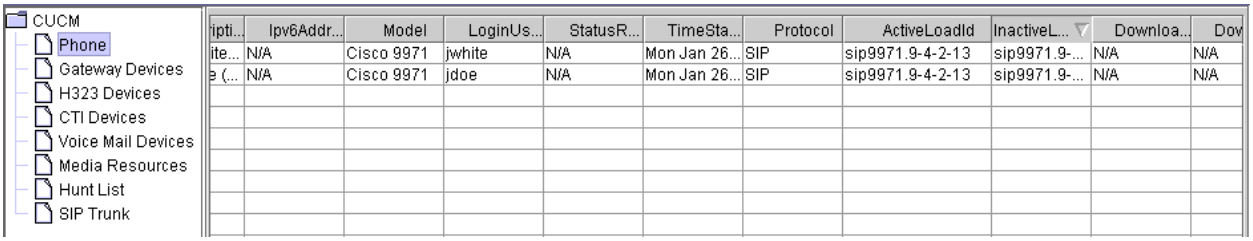


Step 32

Verify that the search is configured to display any status. Click **Next** three times and then click **Finish** to start the search query.

Step 33

In the ActiveLoadid column, obtain the version of the phone load from HQ Phone 1 and note it in the table.



Activity Verification

You have completed this task when you attain this result:

The values were noted in the table at the beginning of this task.

Work with Profiles

In this task, you will use the Cisco Unified RTMT to create two profiles that can be loaded when the program starts. The first profile, which you will name CUCM, should monitor Cisco Unified Communications Manager parameters, the current call activity, and the device summary in two different tabs. The second profile, which you will name system, should monitor the percent usage of the common and active partition, the percent CPU time for both processors, and the percent virtual memory. For the second profile, use a polling rate of 5 seconds.

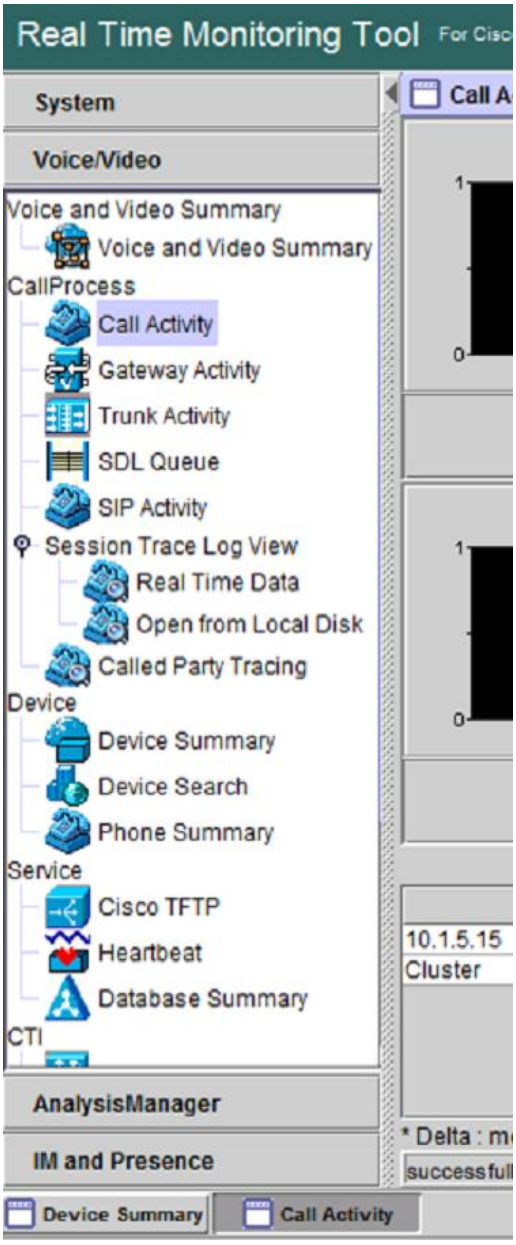
Complete these steps:

Step 34

Click in the monitor pane on an open category (tab at the bottom, for example, Device Search) and choose **Close All Windows** to start with an empty screen.

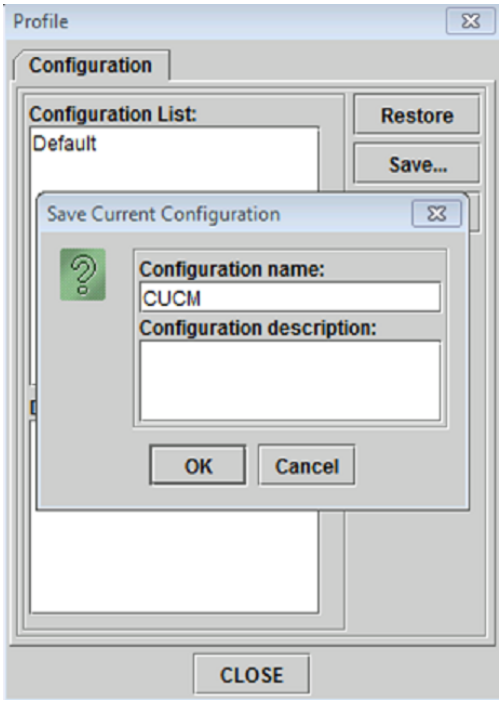
Step 35

From the Voice/Video submenu, open **Call Activity** and **Device Summary**. Both tabs should now be open in the monitoring pane (shown in the bottom of the screen).



Step 36

Navigate to **File > Profile** and click **Save**. Enter **CUCM** as the configuration name and click **OK**. Close the profile window.



Step 37

Click again in the monitor pane on an open category and choose **Close All Windows**.

Step 38

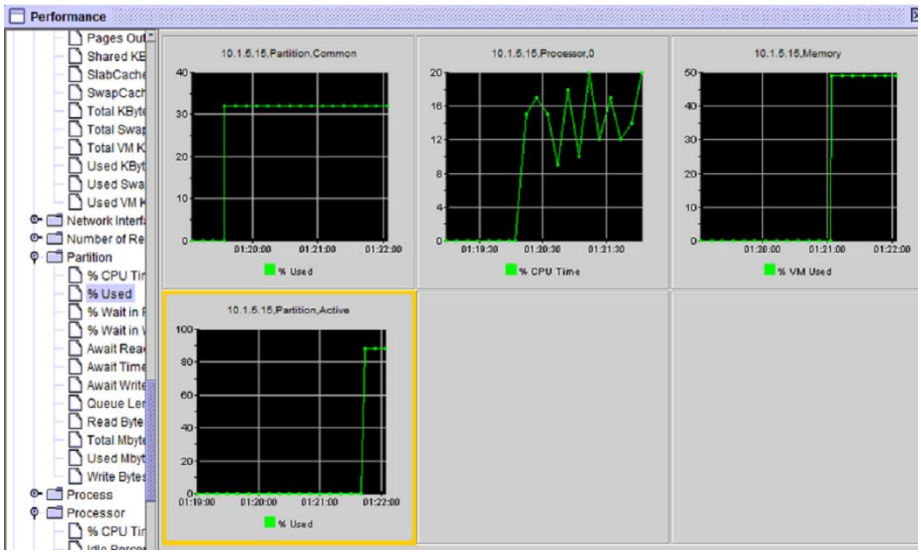
In the System > Performance category, navigate to **10.1.5.15 > Partition > % Used**. Drag and drop the **% Used** counter to the first of the six free charts. From the Object Instances window, choose **Common** and click **Add**. Choose the **% Used** counter again and choose **Active** from the Object Instances window.

Step 39

Navigate to **10.1.5.15 > Processor > % CPU Time**. Drag and drop the **% CPU Time** counter to the next free chart. From the Object Instances window, choose **0** to choose the first CPU.

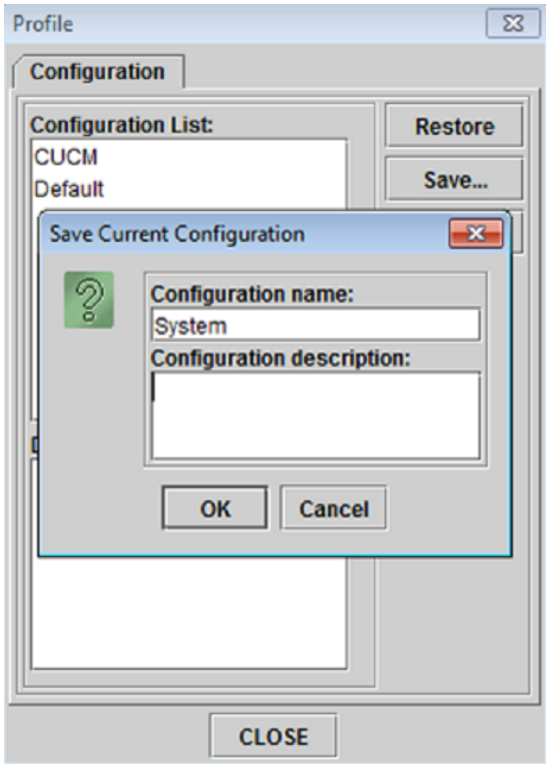
Step 40

To display the percent of used virtual memory, navigate to **10.1.5.15 > Memory > % VM Used**. Drag and drop the **% VM Used** counter to the next free chart. The performance category should display four different counters.



Step 41

To save the view in a profile, navigate to **File > Profile** and click **Save**. Use **System** as the configuration name. Click **OK** and close the profile window.



Step 42

To test the profiles, navigate to **File > Profile**. From the Configuration list, choose **System** and click **Restore**. The four previously monitored counters are displayed again.

Step 43

Repeat the previous step with the profile **CUCM**.

Step 44

Close the RTMT tool.

Activity Verification

You have completed this task when you attain this result:

Two profiles were created and can be selected.