Full Time Recording (CTI)
FTR 3

Installation and Administration Guide

Dec 2018

Doc version 3a

Atea Systems Limited
PO Box 22042, 2 Ganges Road
Khandallah, Wellington, New Zealand
NZBN 9429036367115

Atea Systems Pty Limited
PO Locked Bag Q800, QVB Post Office
Sydney, NSW 1230, Australia
ABN 57 122 952 783

Contents

Document History

Date	Author	Version	Summary
7/12/2018	Murray Lum	3a	Now uses CTI control to bridge the voice streams rather than a SIP call
4/05/2016	Murray Lum	2.5e	New SIP timer settings and update for 2.5.00 Increase default disk size to 150MB New settings to increase SIP session expiry, and disable G.729 silence suppression Added instructions for backups and alerting
24/04/2015	Murray Lum	2.5	Updated for release 2.2.40, removed APEX section, changed install to VM import, expanded management of phones and licenses
25/09/2012	Te Kairangi Katene	2.4	Removed cdr references for cm 8.5+
15/09/2010	Jamie Brown	2.3	Updated APEX section
16/08/2010	Jamie Brown	2.2	Updated section SIP Trucks
26/07/2010	Jamie Brown	2.1	Updated section on managing recordings
16/07/2010	Jamie Brown	2	Updated diagrams and troubleshooting
17/06/2010	Jamie Brown	1.0	Initial administration guide

Related Documents

Document	Description
FTR User guide	User guide

1. Purpose of this guide – FTR installation and UCM config

This guide describes the administrative tasks to configure and maintain the Atea Full Time Recording (FTR) application. This uses CTI control of the device Built-in-Bridge (BIB) to stream audio to the recorder.

This document covers:

- FTR overview
- FTR VM appliance installation (pre-configured instance supplied by Atea)
- UCM configuration for the FTR application
- Recording file basic management
- Troubleshooting tips

For additional information on configuring the Cisco UCM, please see the Cisco documentation.

2. Product Overview

In BIB based call recording, recording streams get forked from agent phone device to the recorder. When a call is established, the CUCM notifies the recorder. In turn the recorder gets the device to set up a monitoring session using BIB and stream this to the recorder. This uses the Cisco monitoring API.

The recorded device must have the built-in-bridge feature.

The steps for establishing a recording session are:

1. The agent makes a call or someone calls them
2. The CUCM lets the recorder know about the call using the CTI connection
3. The recorder tells the agent phone device to use the built-in-bridge to stream the media to the recorder
4. The recorder receives the stream and saves the audio as a file.

To record conversations, the agent devices are listed on the FTR recorder.

3. Supplied Software

The Atea FTR server appliance is usually supplied as a virtual machine using OVF or OVA files(s). This VM may be set up as a separate appliance independent of other Atea supplied applications. The resource availability can be critical for the recording appliance.

Virtual Machine guest resources

Item	Resources
Processor	2 virtual CPUs (2.1GHz min) 64-bit
RAM	4GB
Disk	150GB HDD (Resilient data store recommended)
Additional disk for recordings	Usually greater than 150GB HDD – depending on recording retention requirements. See the section on recording files for a sizing table. Recording consumes 480kB per minute.

4. Installing and Configuring FTR recording

4.1. Pre-requisites

Here's what you'll need before you begin:

- Access to the CUCM to configure the CTI resources
- Virtual machine resources for the FTR VM (pre-configuration of VM host is **not** required)
- The VM OVF (or OVA) files supplied by Atea
- A back-up and restoration strategy for the server
- An archive strategy for the recordings
- A remote access mechanism to allow Atea Support to configure and support the appliance.

To allow Atea to create the VM please supply the information below to support@ateasystems.com, using the form at https://www.ateasystems.com/virtual-server-config/

- hostname
- IP-address (& mask & gateway)
- DNS details
- NTP IP-address
- SMTP IP-address

Forward any security documentation to support@ateasystems.com.

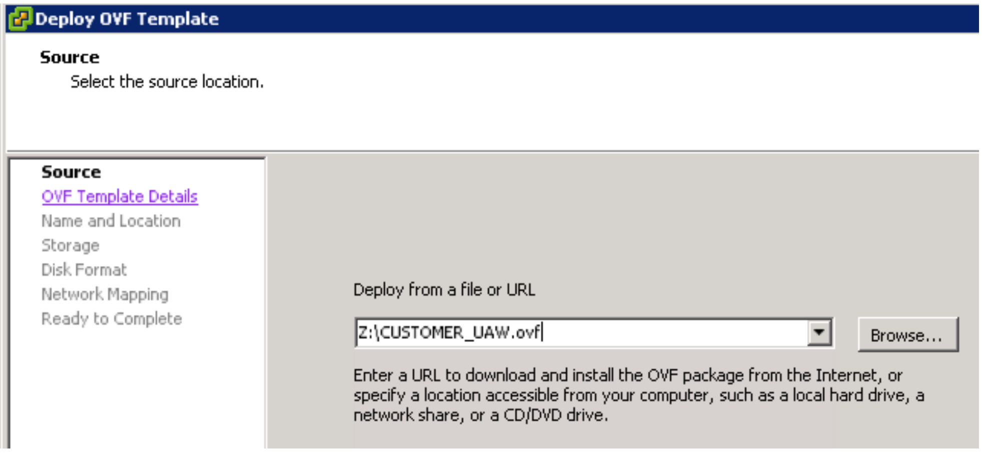
Information required later to setup and generate a license file:

- Server MAC address.

4.2. Install the Virtual Machine

We normally supply the Atea FTR as a virtual machine, shipped in OVF format. Download and check the files provided.

1. From your preferred client (such as the vSphere Client), navigate to "**Deploy OVF Template**"
2. Browse to the location where the downloaded files are stored and select the [filename].ovf (or .ova)



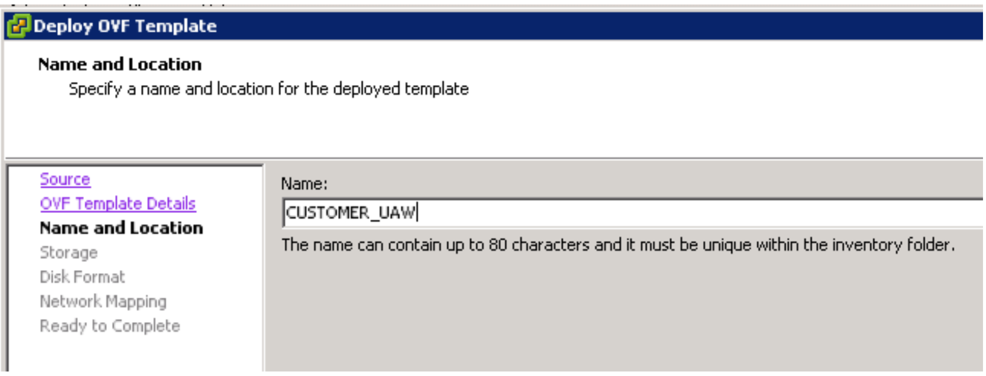
Source
Select the source location.

Deploy from a file or URL

Z:\CUSTOMER_UAW.ovf

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

3. Enter a **name** for the instance

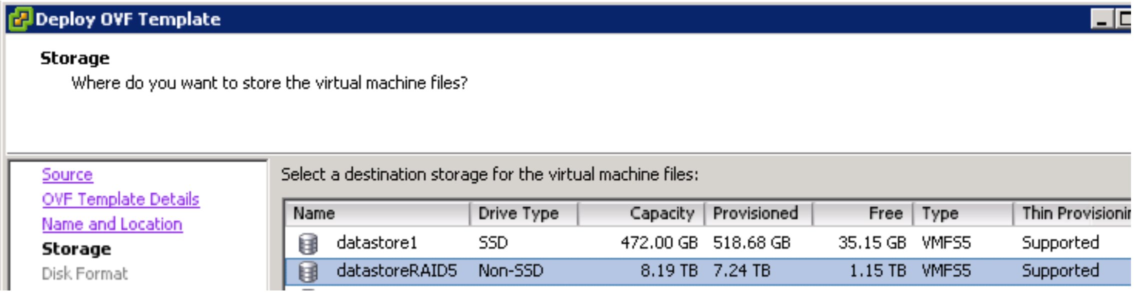


Name and Location
Specify a name and location for the deployed template

Name:
CUSTOMER_UAW

The name can contain up to 80 characters and it must be unique within the inventory folder.

4. Select the data-store where you want the VM guest to reside

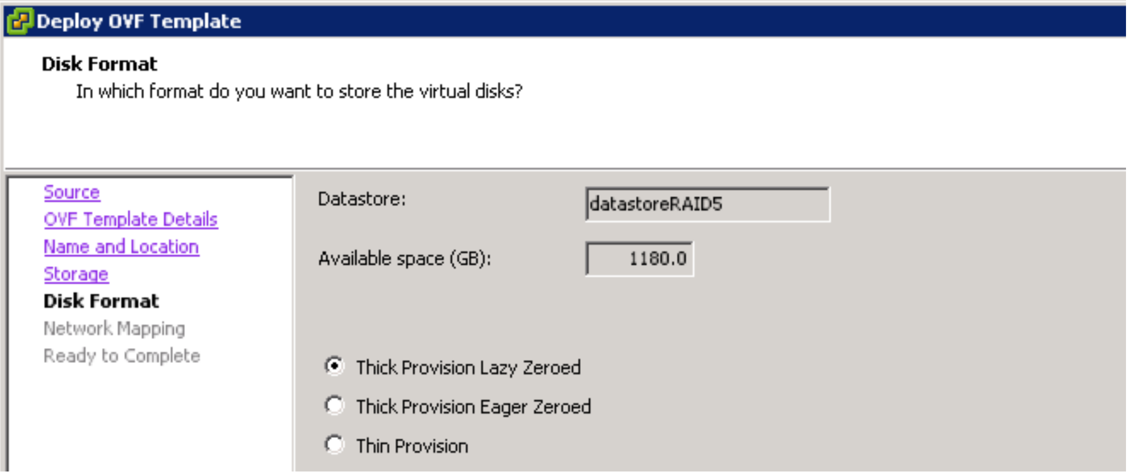


Storage
Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisionir
datastore1	SSD	472.00 GB	518.68 GB	35.15 GB	VMFS5	Supported
datastoreRAID5	Non-SSD	8.19 TB	7.24 TB	1.15 TB	VMFS5	Supported

5. Select the **Disk Format** (*Thick Provision is recommended*)



Disk Format

In which format do you want to store the virtual disks?

Datastore: datastoreRAID5

Available space (GB): 1180.0

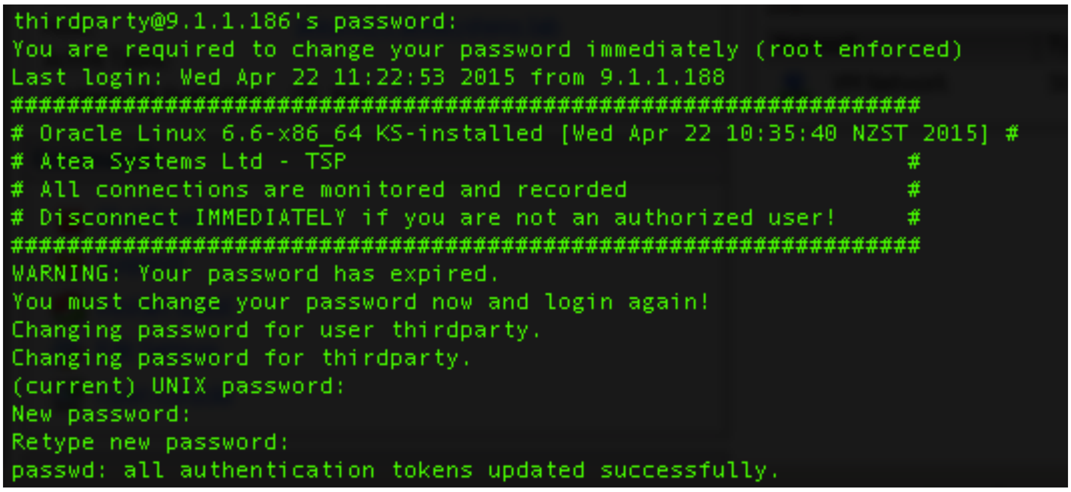
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

6. Start the server instance (**Power On**)

7. Log into the console with user: **thirdparty**, and the password provided. You must change the password on first login. Enter the old password again, then the new password twice.



```
thirdparty@9.1.1.186's password:
You are required to change your password immediately (root enforced)
Last login: Wed Apr 22 11:22:53 2015 from 9.1.1.188
#################################################################
# Oracle Linux 6.6-x86_64 KS-installed [Wed Apr 22 10:35:40 NZST 2015] #
# Atea Systems Ltd - TSP                                        #
# All connections are monitored and recorded                    #
# Disconnect IMMEDIATELY if you are not an authorized user!     #
#################################################################
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user thirdparty.
Changing password for thirdparty.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

This confirms that you have access to the VM in the future for maintenance.

You may now set up both the server backup and remote access for Atea support.

4.3. Configure backups

The automatic backup cycle runs daily at 11pm.

The components backed up locally on the servers are:

- Linux configuration (7 days kept with day of week indicator from 1 to 7)
- Atea applications (7 days kept)
- Atea application properties (7 days kept)
- Oracle database (2 days kept)

We suggest that sFTP is used to copy the application and database backups to a network location.

The procedure to enable the sFTP copying is (see also the Atea website):

ssh thirdparty@ateaserver-ip-address

sudo su -

vim /etc/atea/scripts/sftpBackup.sh (enter the sftp server details)

Change the host, user, password and path parameters on lines 4-7

vim /etc/atea/scripts/fullBackup.sh (change line 23, DO_BACKUP_COPY=true)

Now check that the ssh rsa key is stored and connectivity is okay by connecting to the sftp server

sftp user@sftpserver (enter password to establish connection)

exit

4.4. Configure alerting

A monitor script runs every 10 mins by default and sends alerts if certain conditions are met. These may include CPU, IOWAIT, Free disk and memory and whether the application can connect to the Oracle database.

To change the monitor script to send alerts to your service provider, you'll need to modify the script:

ssh thirdparty@ateaserver-ip-address

sudo su -

vim /etc/atea/scripts/monitor.sh

Change the MAILTO and MAILFROM lines with the Service-Provider specific email addresses.

5. Configure the CUCM for Recording

5.1. Communication requirements

The FTR and UCM have several communication streams. These are:

- AXL for user information and settings

- CTI for call status information and recording calls (uses Cisco monitoring API and phones must have built-in-bridge BIB)

Here's the UCM configuration requirements:

1. **FTR Users** – these are users that can listen to FTR recordings. They must be a member of the CUCM group [Atea_FTR_User***] to gain access. An FTR administrator assigns which groups they belong to and hence what recordings they have access to.
2. **FTR Administrators –** these are users who can administer the FTR. They must be a member of the CUCM group [Atea_FTR_Admin***]. The administrators set which devices are to be recorded and which group the device belongs to. They also set which group a user belongs to (so that a user only has access to the recordings from their group).
3. **Atea FTR** makes queries and requests via number of UCM APIs. It uses a UCM account with these settings:
    a. Serviceability
    b. AXL
    c. CTI (JTAPI) including a CTI Route Point and Port

Note: The screenshots and menu items in this guide are for Cisco UCM version 10.0. Other versions may be different.

The basic tasks to configure the UCM are:

1. Assign SCM Administrator Privileges
2. Setup the application user for API access
3. Setup the phone devices to enable the built-in bridge monitoring

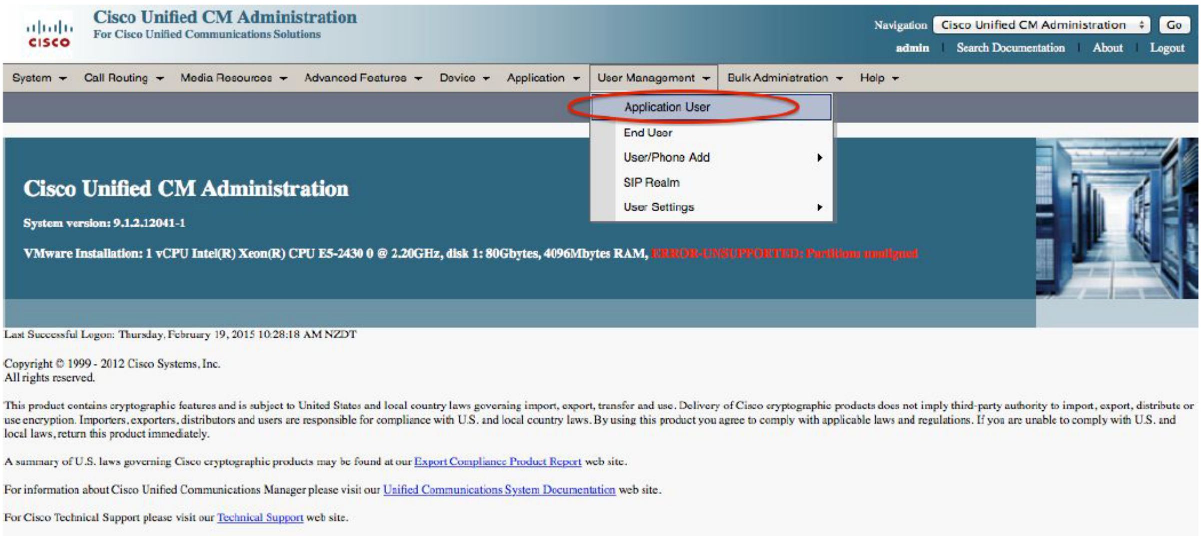
6. Setup Application Account for API Access

The ATEA SCM requires an application user to access several Cisco UCM APIs.

In this section, we'll:

- Create an **Application User** named **ATEA_FTR**
- Create an **Access Control Group** named **ATEA_FTR_API** and add roles
- Give **ATEA_FTR** a **CTI Route Point** as an associated controlled device
- Give **ATEA_FTR** a **CTI Port** as an associated controlled device

1. Create the Application user. In UCM Administration, go to **User Management** > **Application User**



Cisco Unified CM Administration

System version: 9.1.2.12041-1

VMware Installation: 1 vCPU Intel(R) Xeon(R) CPU E5-2430 0 @ 2.20GHz, disk 1: 80Gbytes, 4096Mbytes RAM, ERROR-UNSUPPORTED: Partitions unaligned

Last Successful Logon: Thursday, February 19, 2015 10:28:18 AM NZDT

Copyright © 1999 - 2012 Cisco Systems, Inc.
All rights reserved.

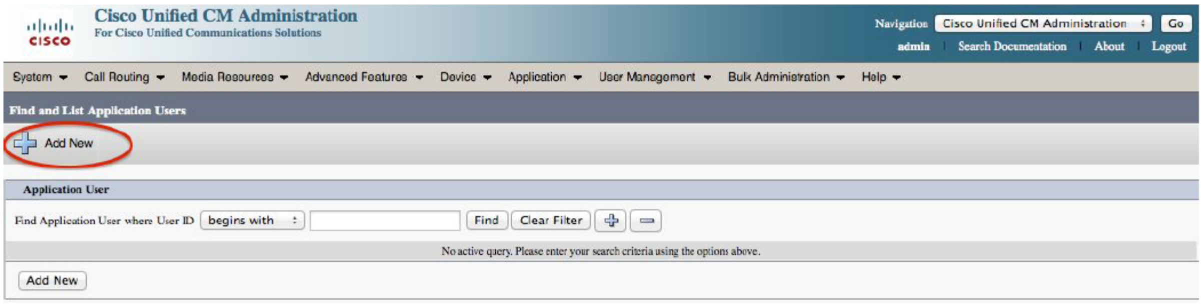
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors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

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

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

2. Click **Add New**



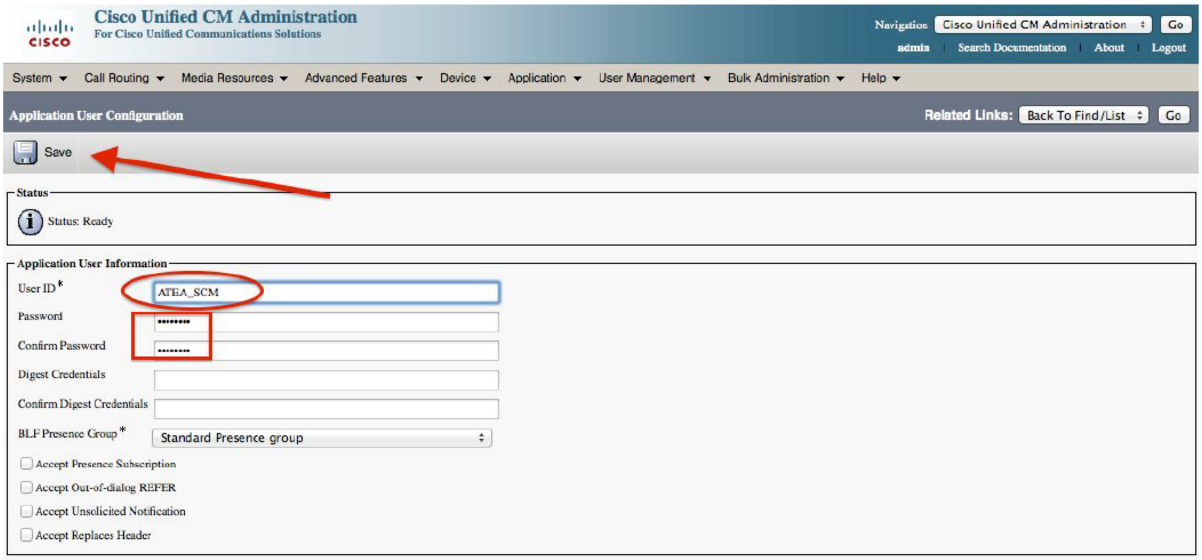
Find and List Application Users

Application User

Find Application User where User ID begins with

No active query. Please enter your search criteria using the options above.

3. Enter the **User ID ATEA_FTR** and **password** (twice), then click **Save**


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Related Links: Back To Find/List Go
Save

Application User Configuration

Status

Status: Ready

Application User Information

User ID *	ATEA_SCM
Password	••••••••
Confirm Password	••••••••
Digest Credentials	
Confirm Digest Credentials	
BLF Presence Group *	Standard Presence group

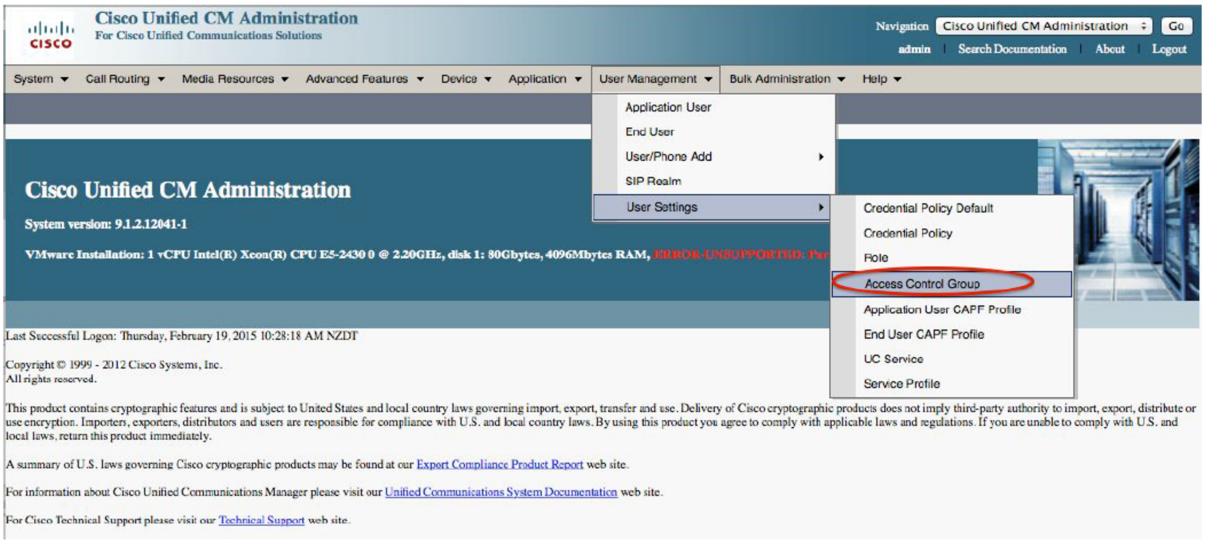
□ Accept Presence Subscription

□ Accept Out-of-dialog REFER

□ Accept Unsolicited Notification

□ Accept Replaces Header

4. Now create an Access Control Group named ATEA_SCM_API. Go to **User Management** > **User Settings** > **Access Control Group**


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Application User
End User
User/Phone Add
SIP Realm
User Settings
Credential Policy Default
Credential Policy
Role
Access Control Group
Application User CAPF Profile
End User CAPF Profile
UC Service
Service Profile

Cisco Unified CM Administration

System version: 9.1.2.12041-1

VMware Installation: 1 vCPU Intel(R) Xeon(R) CPU E5-2430 0 @ 2.20GHz, disk 1: 80Gbytes, 4096Mbytes RAM, ERROR-UNSUPPORTED: Pa

Last Successful Logon: Thursday, February 19, 2015 10:28:18 AM NZDT

Copyright © 1999 - 2012 Cisco Systems, Inc.
All rights reserved.

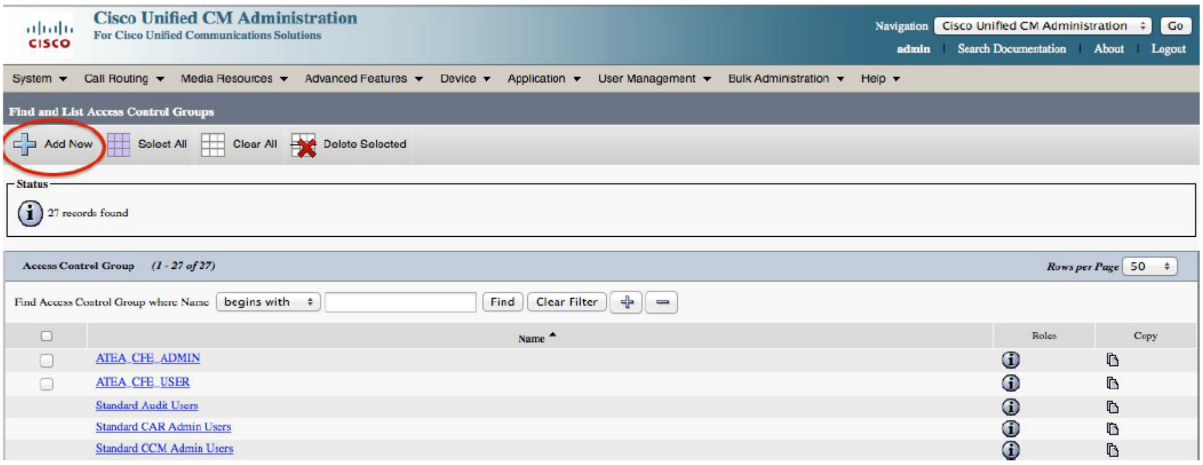
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors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

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

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

5. Click **Add New**


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Add New
Select All
Clear All
Delete Selected
Find
Clear Filter

Find and List Access Control Groups

Status

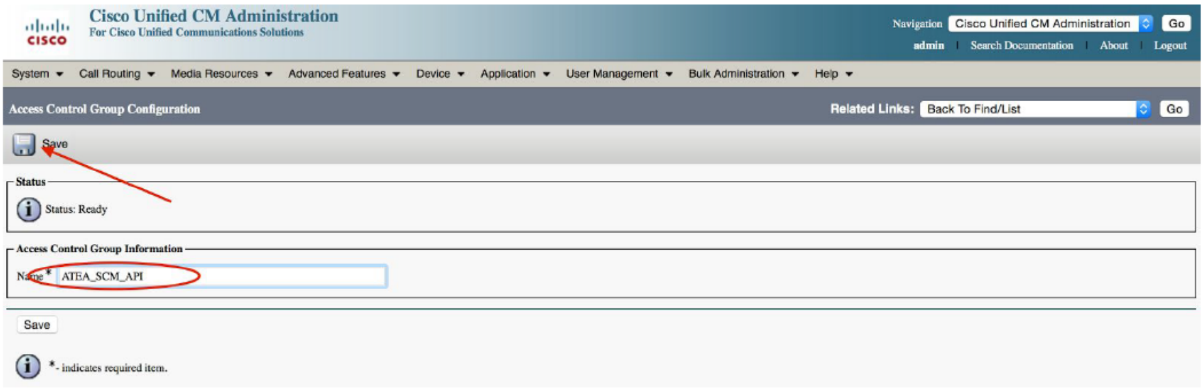
27 records found

Access Control Group (1 - 27 of 27) Rows per Page 50

Find Access Control Group where Name begins with

□	Name ▲	Roles	Copy
□	ATEA_CFE_ADMIN	ⓘ	⎘
□	ATEA_CFE_USER	ⓘ	⎘
	Standard Audit Users	ⓘ	⎘
	Standard CAR Admin Users	ⓘ	⎘
	Standard CCM Admin Users	ⓘ	⎘

6. Enter the **Name ATEA_FTR_API**, then click **Save**


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Access Control Group Configuration
Related Links: Back To Find/List Go
Save

Status

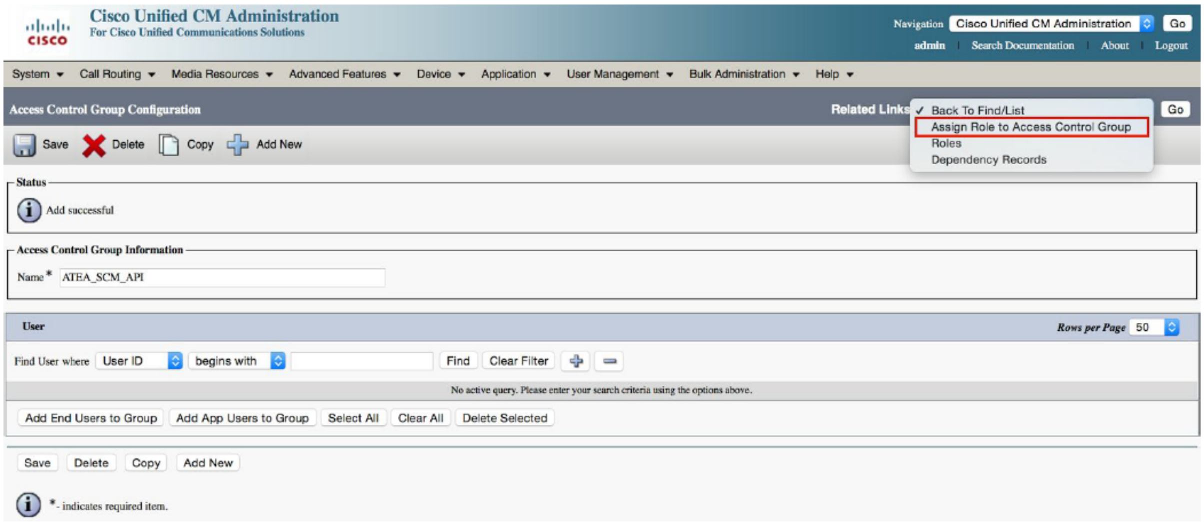
Status: Ready

Access Control Group Information

Name* ATEA_SCM_API

*- indicates required item.

7. Next, let’s assign the roles to this group. For the access control group **ATEA_FTR_API**, select the related link **Assign Role to Access Control Group**.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Access Control Group Configuration
Related Links
✓ Back To Find/List
Assign Role to Access Control Group
Roles
Dependency Records
Go
Save Delete Copy Add New

Status

Add successful

Access Control Group Information

Name* ATEA_SCM_API

User

Rows per Page 50

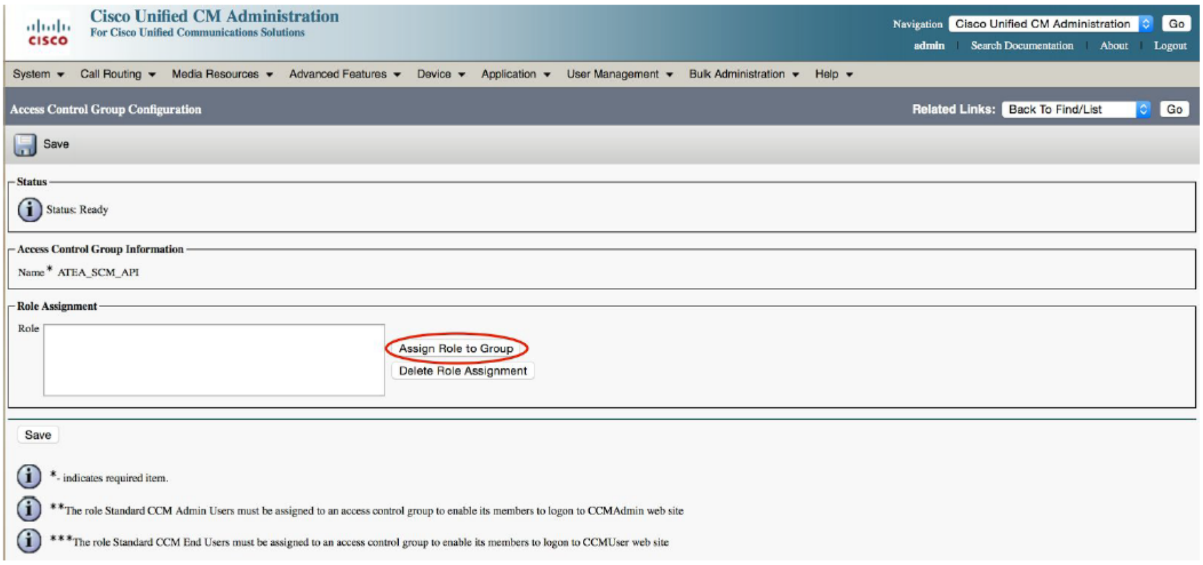
Find User where User ID begins with

No active query. Please enter your search criteria using the options above.

Add End Users to Group Add App Users to Group Select All Clear All Delete Selected
Save Delete Copy Add New

*- indicates required item.

8. Click the button, **Assign Role to Group**


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Access Control Group Configuration
Related Links: Back To Find/List Go
Save

Status

Status: Ready

Access Control Group Information

Name* ATEA_SCM_API

Role Assignment

Role

Assign Role to Group
Delete Role Assignment
Save

*- indicates required item.

**The role Standard CCM Admin Users must be assigned to an access control group to enable its members to logon to CCMAdmin web site

***The role Standard CCM End Users must be assigned to an access control group to enable its members to logon to CCMUser web site

9. Click **Find**. From the results, select the access control group roles as shown in the screenshots below, then click **Add Selected**.

   Add these roles:

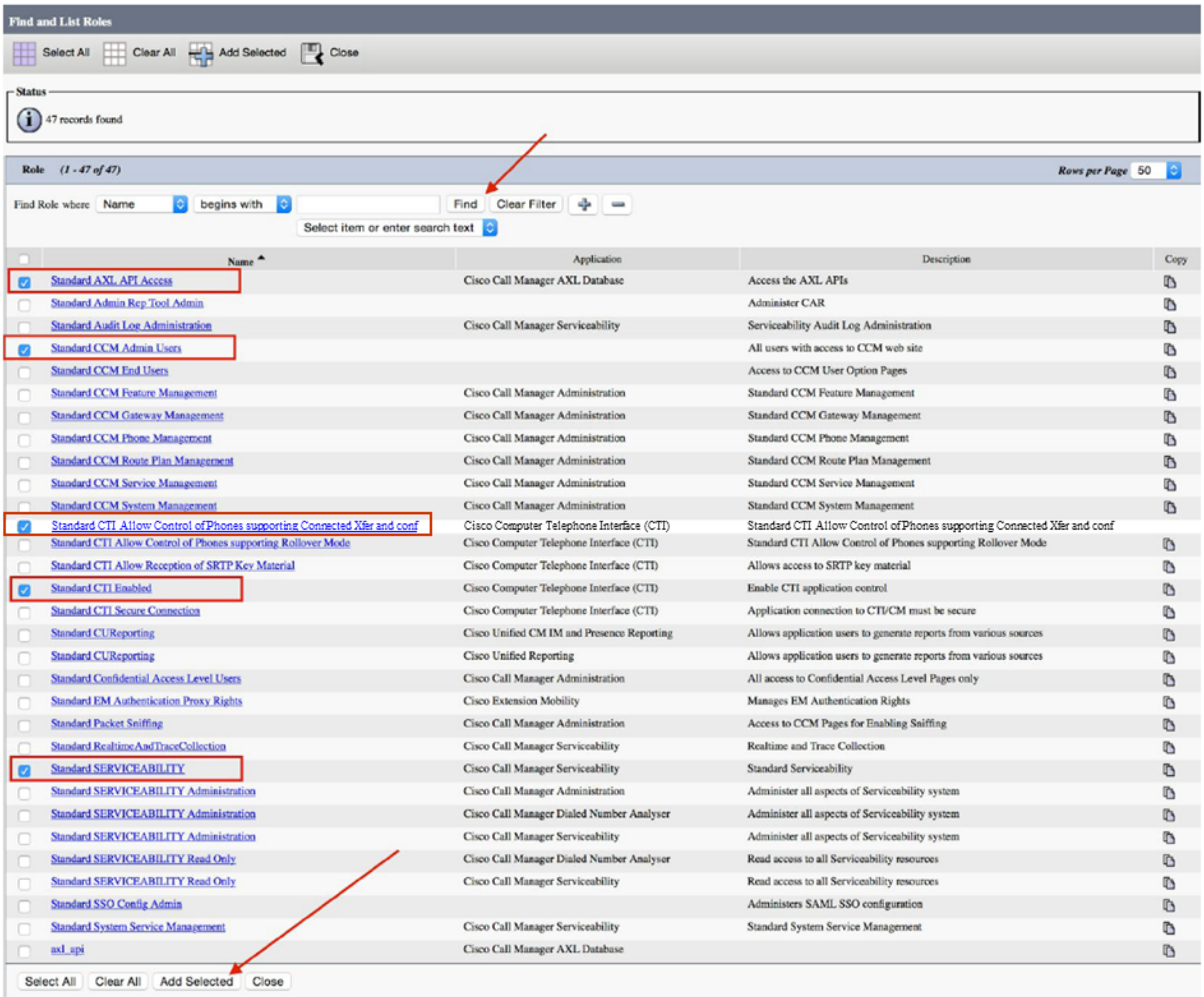
   a. Standard AXL API Access

   b. Standard CCM Admin Users

   c. Standard CTI Allow Control of Phones supporting Connected Xfer and conf

   d. Standard CTI enabled

   e. Standard SERVICEABILITY



Find and List Roles

Status

47 records found

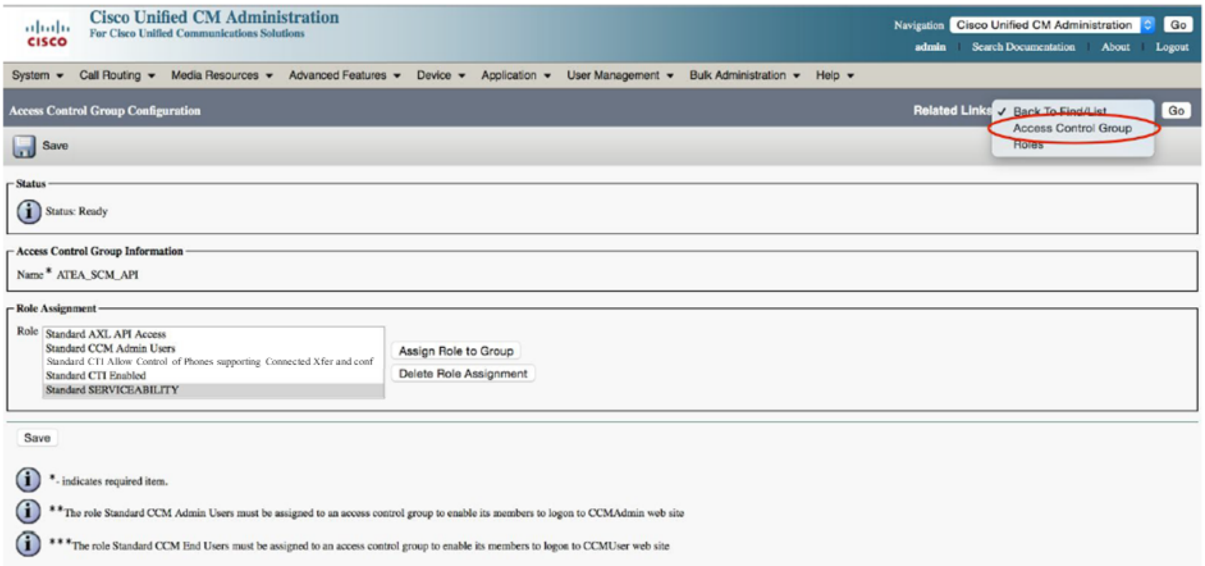
Role (1 - 47 of 47) Rows per Page 50

Find Role where Name begins with

Select item or enter search text

□	Name	Application	Description	Copy
☑	Standard AXL API Access	Cisco Call Manager AXL Database	Access the AXL APIs	⎘
□	Standard Admin Rep Tool Admin		Administer CAR	⎘
□	Standard Audit Log Administration	Cisco Call Manager Serviceability	Serviceability Audit Log Administration	⎘
☑	Standard CCM Admin Users		All users with access to CCM web site	⎘
□	Standard CCM End Users		Access to CCM User Option Pages	⎘
□	Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management	⎘
□	Standard CCM Gateway Management	Cisco Call Manager Administration	Standard CCM Gateway Management	⎘
□	Standard CCM Phone Management	Cisco Call Manager Administration	Standard CCM Phone Management	⎘
□	Standard CCM Route Plan Management	Cisco Call Manager Administration	Standard CCM Route Plan Management	⎘
□	Standard CCM Service Management	Cisco Call Manager Administration	Standard CCM Service Management	⎘
□	Standard CCM System Management	Cisco Call Manager Administration	Standard CCM System Management	⎘
☑	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	Cisco Computer Telephone Interface (CTI)	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	
□	Standard CTI Allow Control of Phones supporting Rollover Mode	Cisco Computer Telephone Interface (CTI)	Standard CTI Allow Control of Phones supporting Rollover Mode	⎘
□	Standard CTI Allow Reception of SRTP Key Material	Cisco Computer Telephone Interface (CTI)	Allows access to SRTP key material	⎘
☑	Standard CTI Enabled	Cisco Computer Telephone Interface (CTI)	Enable CTI application control	⎘
□	Standard CTI Secure Connection	Cisco Computer Telephone Interface (CTI)	Application connection to CTI/CM must be secure	⎘
□	Standard CUReporting	Cisco Unified CM IM and Presence Reporting	Allows application users to generate reports from various sources	⎘
□	Standard CUReporting	Cisco Unified Reporting	Allows application users to generate reports from various sources	⎘
□	Standard Confidential Access Level Users	Cisco Call Manager Administration	All access to Confidential Access Level Pages only	⎘
□	Standard EM Authentication Proxy Rights	Cisco Extension Mobility	Manages EM Authentication Rights	⎘
□	Standard Packet Sniffing	Cisco Call Manager Administration	Access to CCM Pages for Enabling Sniffing	⎘
□	Standard RealtimeAndTraceCollection	Cisco Call Manager Serviceability	Realtime and Trace Collection	⎘
☑	Standard SERVICEABILITY	Cisco Call Manager Serviceability	Standard Serviceability	⎘
□	Standard SERVICEABILITY Administration	Cisco Call Manager Administration	Administer all aspects of Serviceability system	⎘
□	Standard SERVICEABILITY Administration	Cisco Call Manager Dialed Number Analyser	Administer all aspects of Serviceability system	⎘
□	Standard SERVICEABILITY Administration	Cisco Call Manager Serviceability	Administer all aspects of Serviceability system	⎘
□	Standard SERVICEABILITY Read Only	Cisco Call Manager Dialed Number Analyser	Read access to all Serviceability resources	⎘
□	Standard SERVICEABILITY Read Only	Cisco Call Manager Serviceability	Read access to all Serviceability resources	⎘
□	Standard SSO Config Admin		Administers SAML SSO configuration	⎘
□	Standard System Service Management	Cisco Call Manager Serviceability	Standard System Service Management	⎘
□	axl_api	Cisco Call Manager AXL Database		⎘

10. Click **Save** and then select **Access Control Group** from the drop-down list at the top right, and click **Go**.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Access Control Group Configuration
Related Links: Back To Find/List Access Control Group Roles Go
Save
Assign Role to Group
Delete Role Assignment
Save

Status

Status: Ready

Access Control Group Information

Name* ATEA_SCM_API

Role Assignment

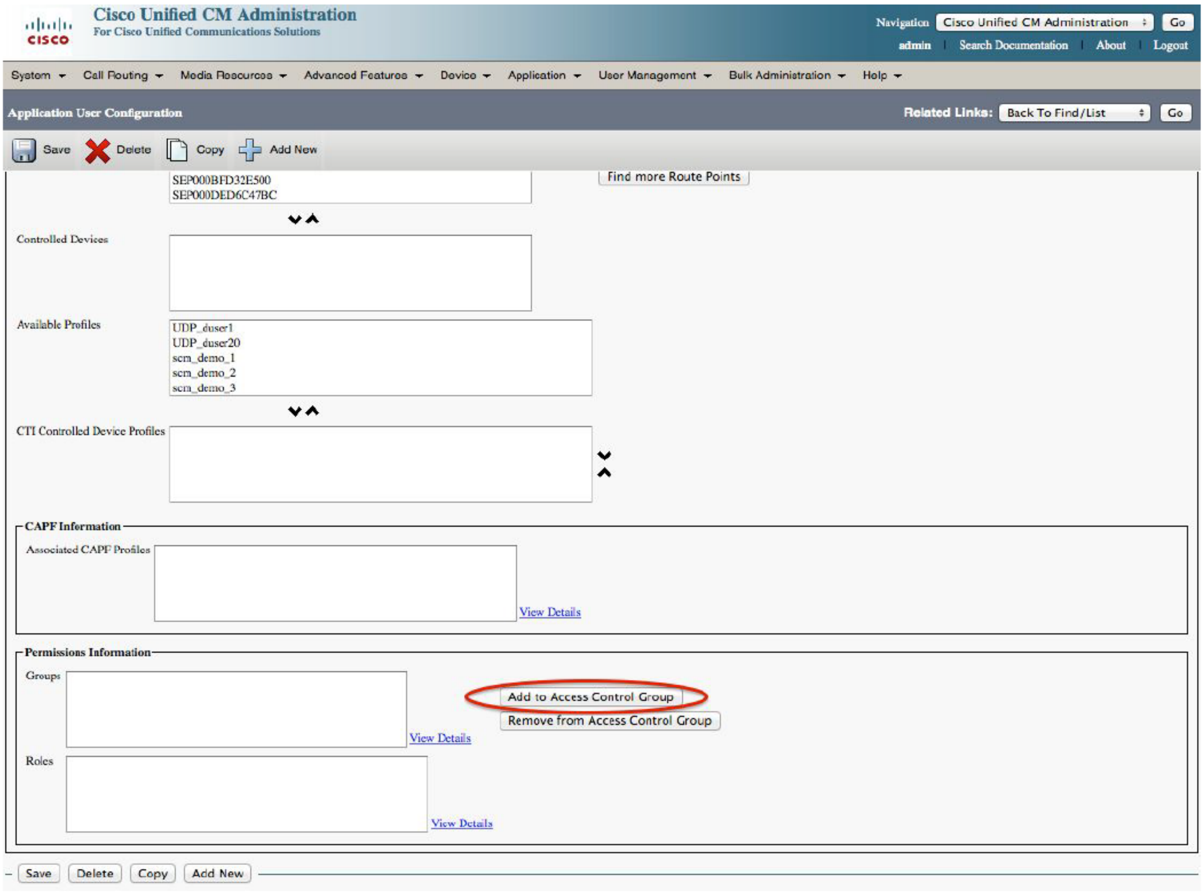
Role Standard AXL API Access
Standard CCM Admin Users
Standard CTI Allow Control of Phones supporting Connected Xfer and conf
Standard CTI Enabled
Standard SERVICEABILITY

*- indicates required item.

**The role Standard CCM Admin Users must be assigned to an access control group to enable its members to logon to CCMAdmin web site

***The role Standard CCM End Users must be assigned to an access control group to enable its members to logon to CCMUser web site

11. Now that we've created the Access Control Group, assign it to the application user we created earlier. Navigate back to the application user (ATEA_FTR) under **User Management** > **Application User**, scroll to the bottom of the page, and click **Add to Access Control Group**


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Application User Configuration
Related Links: Back To Find/List Go
Save Delete Copy Add New
Find more Route Points
View Details
Add to Access Control Group
Remove from Access Control Group
View Details
View Details
Save Delete Copy Add New

SEP000BFD32E500
SEP000DED6C47BC

Controlled Devices

Available Profiles UDP_duser1
UDP_duser20
scm_demo_1
scm_demo_2
scm_demo_3

CTI Controlled Device Profiles

CAPF Information

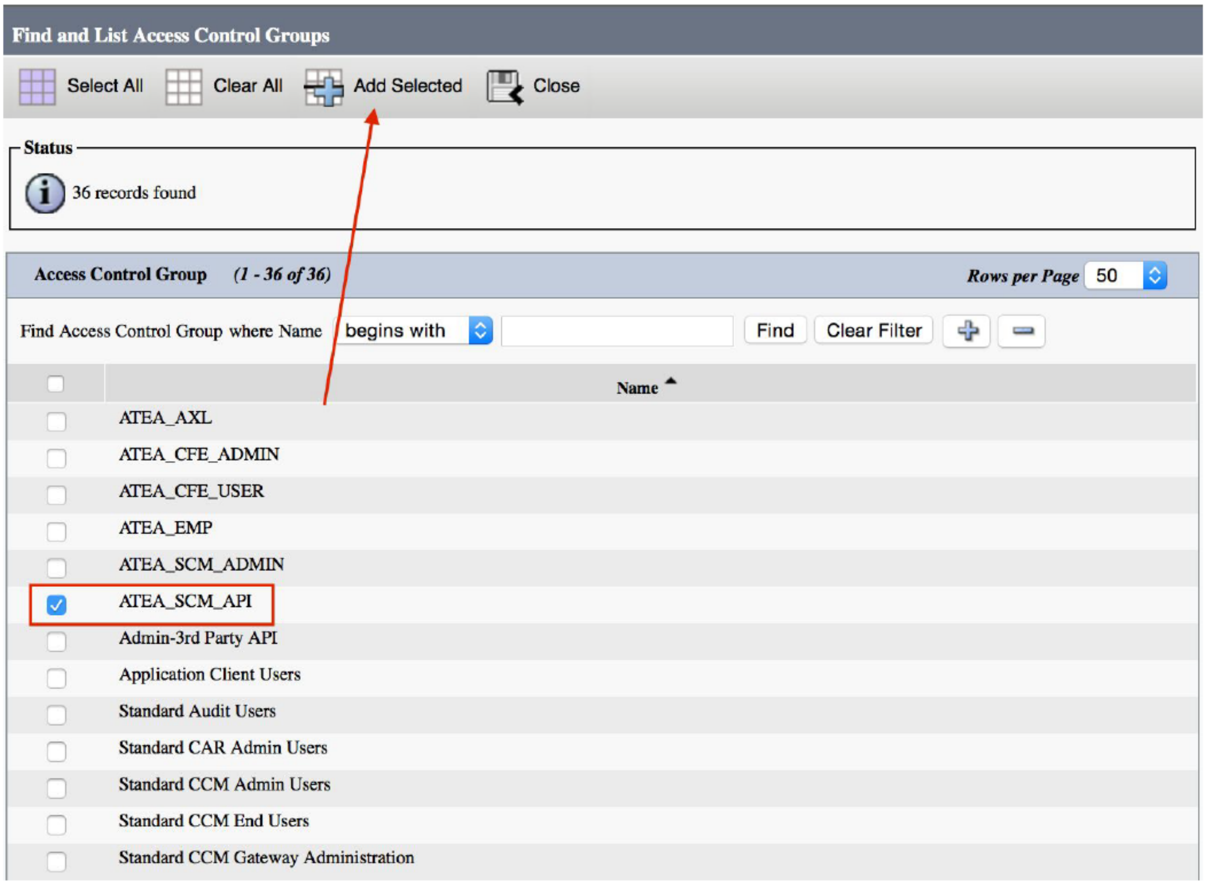
Associated CAPF Profiles

Permissions Information

Groups

Roles

12. A window pops up showing all the **Access Control Groups.** Select **ATEA_FTR_API** then click **Add Selected**



Find and List Access Control Groups

Status

36 records found

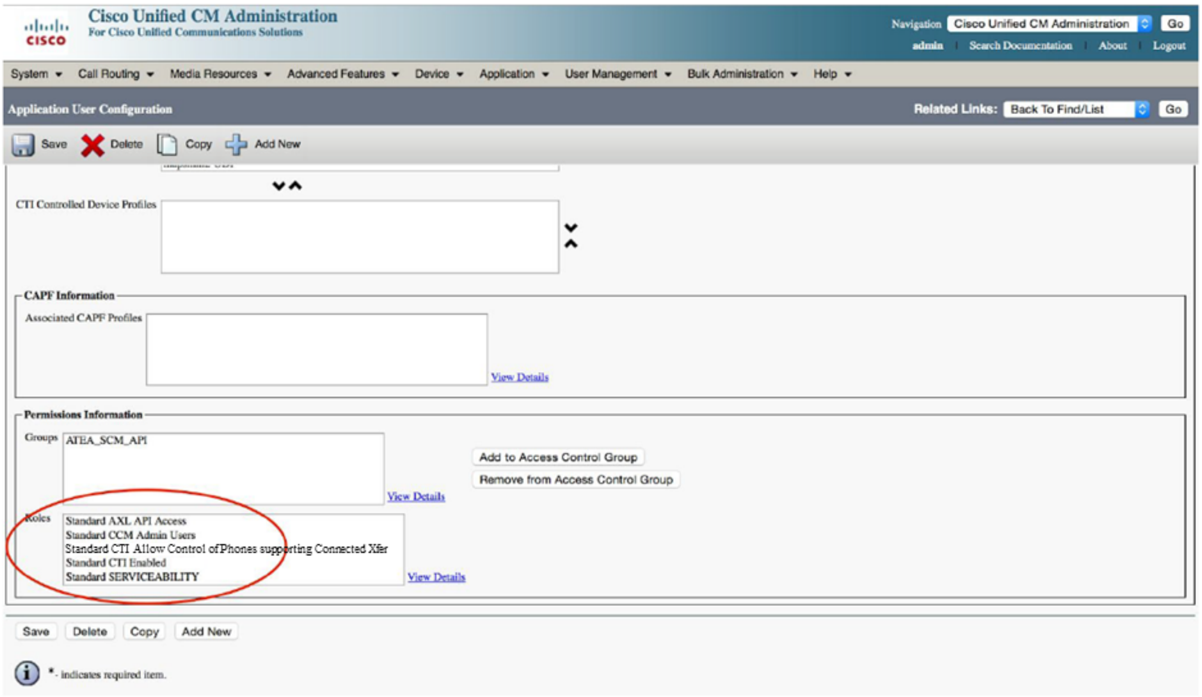
Access Control Group (1 - 36 of 36)

Rows per Page 50

Find Access Control Group where Name begins with

	Name
□	ATEA_AXL
□	ATEA_CFE_ADMIN
□	ATEA_CFE_USER
□	ATEA_EMP
□	ATEA_SCM_ADMIN
☑	ATEA_SCM_API
□	Admin-3rd Party API
□	Application Client Users
□	Standard Audit Users
□	Standard CAR Admin Users
□	Standard CCM Admin Users
□	Standard CCM End Users
□	Standard CCM Gateway Administration

13. Click **Save**. When the page refreshes you should be able to scroll to the bottom and see the newly assign group and roles.



Application User Configuration

CTI Controlled Device Profiles

CAPF Information

Associated CAPF Profiles

Permissions Information

Groups: ATEA_SCM_API

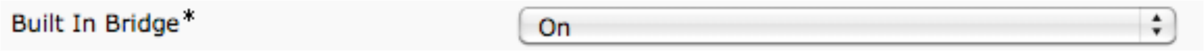
Roles:
Standard AXL API Access
Standard CCM Admin Users
Standard CTI Allow Control ofPhones supporting Connected Xfer
Standard CTI Enabled
Standard SERVICEABILITY

*- indicates required item.

7. Phone settings

7.1. Turn on the built-in bridge on the phone

For each phone to be recorded, enable the built-in bridge. This is enabled on the device itself. On the phone configuration screen in the CUCM administration set “Built In Bridge” to “On”.



Built In Bridge*	On

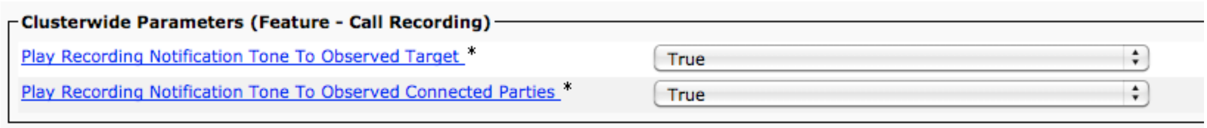
7.2. Allow CTI control for user

[TK to send screenshots]

7.3. Enable the recording tone (optional) [???]

You can set a tone to be played during calls to indicate that the call is being recorded. To enable this, **turn on** the notification tone cluster parameter (the default is off) and the setting on each individual phone.

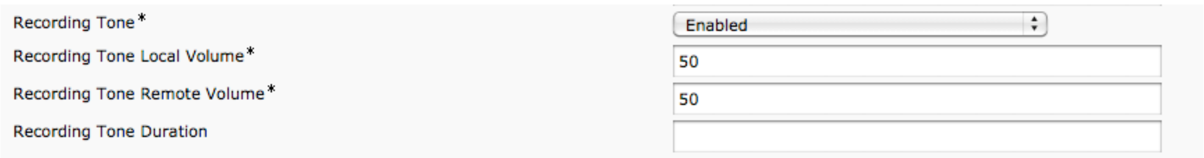
1. Set the cluster wide service parameter to play the recording tone. From the CUCM administration, select the Cisco Call Manager service and scroll down to the call recording feature.
   Set “**Play Recording Notification Tone**” parameters to **true**.



Clusterwide Parameters (Feature - Call Recording)

Play Recording Notification Tone To Observed Target *	True
Play Recording Notification Tone To Observed Connected Parties *	True

2. Now enable the tone for each phone device. This is done on the device itself, not the individual lines. For information on these settings, refer to the Cisco documentation.



Recording Tone*	Enabled
Recording Tone Local Volume*	50
Recording Tone Remote Volume*	50
Recording Tone Duration	

8. Recording files

8.1. General

Recording files are created in several phases. Initially, the application writes the audio header for the file, and then writes the voice-call data in real-time. When the call ends, the file is closed.

The file type is a wave file with the ".wav" suffix. This type of audio file is playable by most media players. This file type is easily copied and stored. Users may copy the file to their local workstation to listen to it, or if they want to share it with a colleague for evaluation.

The recordings can searched directly from the FTR application.

8.2. Disk allocation for recordings

Recordings are stored on a separate disk mounted to the server that runs the FTR application. The suggested budget for sizing this disk is to allow 480kB per minute of recording. Recordings are stored in an uncompressed format.

Recording duration	Disk budget
1 minute	480 kB
1 hour	28.8 MB
100 hours	2.88 GB
1,000 hours	28.8 GB
10,000 hours	288 GB

8.3. Managing recordings [???]

Recording files are located in the folder specified in the application.

Here is an excerpt from the BibCallRecorder properties file.

Property	Value	Comment
SipCallRecorder.recording_directory	/var/recording/	The path must exist

Recordings are stored separately to the call record database. The database includes a pointer to the file location.

If the recording file is moved to another location the recording will display as "not found" on the call search screen. Restoring the file back to the original folder allows the file to be played or retrieved using the normal screen to access the database.

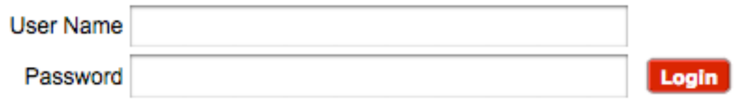
Recordings may be archived or moved manually using operating system commands or other utilities. It is common practice to move or remove older recording files to maintain space on the disk.

9. User Management

9.1. Accessing the FTR landing page – recording supervisors

To connect to the FTR application, use your web browser to navigate to this page –

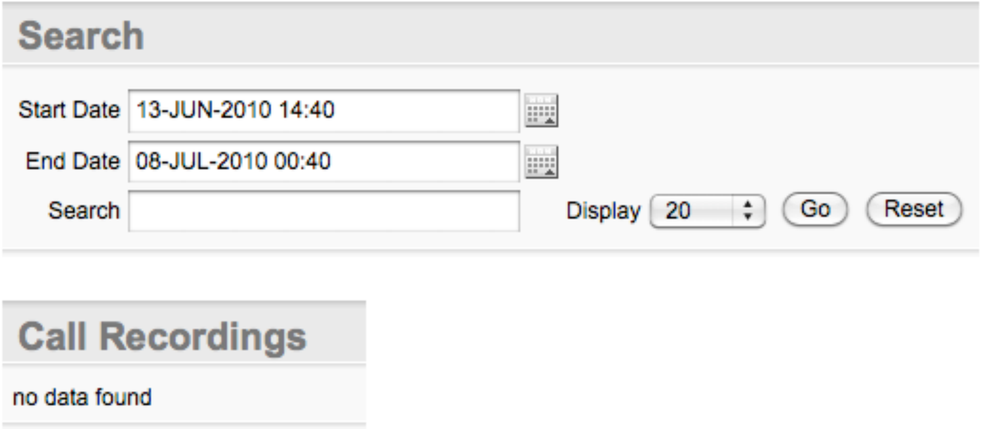
http://[IPaddressOfServer]:8080/apexf?p=103



User Name

Password

Enter the user name and password. This takes you a search screen for the recordings.



Search

Start Date: 13-JUN-2010 14:40

End Date: 08-JUL-2010 00:40

Search

Display: 20

Call Recordings

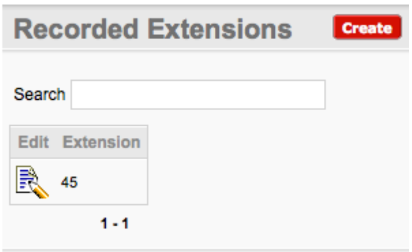
no data found

9.2. Licensing and managing the phones to be recorded

The FTR application is licensed for the number of phones to be recorded. To manage these phones, use a web browser to navigate to this page:

http://[IPaddressOfServer]:8080/apex/f?p=106

This page shows how many licenses are consumed, and the list of phones (DN directory numbers or extensions) to be recorded.

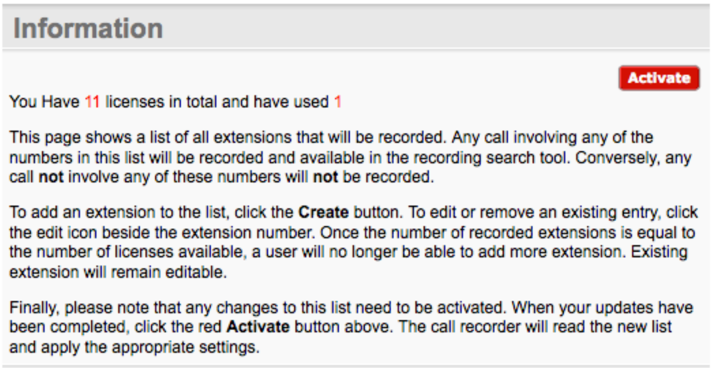


Recorded Extensions

Search

Edit	Extension
✎	45

1 - 1



Information

You Have 11 licenses in total and have used 1

This page shows a list of all extensions that will be recorded. Any call involving any of the numbers in this list will be recorded and available in the recording search tool. Conversely, any call **not** involve any of these numbers will **not** be recorded.

To add an extension to the list, click the **Create** button. To edit or remove an existing entry, click the edit icon beside the extension number. Once the number of recorded extensions is equal to the number of licenses available, a user will no longer be able to add more extension. Existing extension will remain editable.

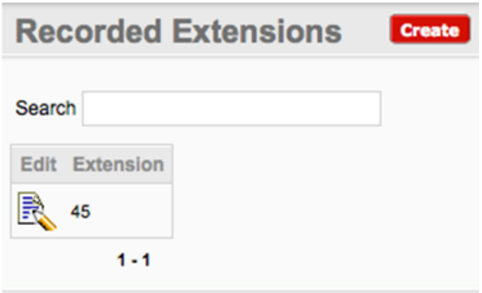
Finally, please note that any changes to this list need to be activated. When your updates have been completed, click the red **Activate** button above. The call recorder will read the new list and apply the appropriate settings.

Note – in order for a phone to be recorded it must be set up in the CUCM with a recording profile, as well as this list.

To change the size of your license, please contact Atea Systems.

To add phones to the list:

1. From the main **Manage Recorded Extensions** page, click the **Create** button to go to the next page



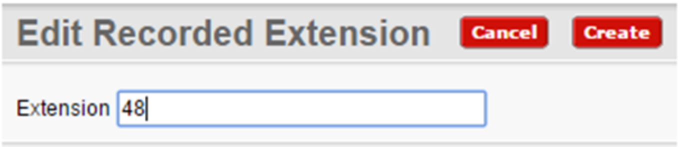
Recorded Extensions

Search

Edit	Extension
✎	45

1 - 1

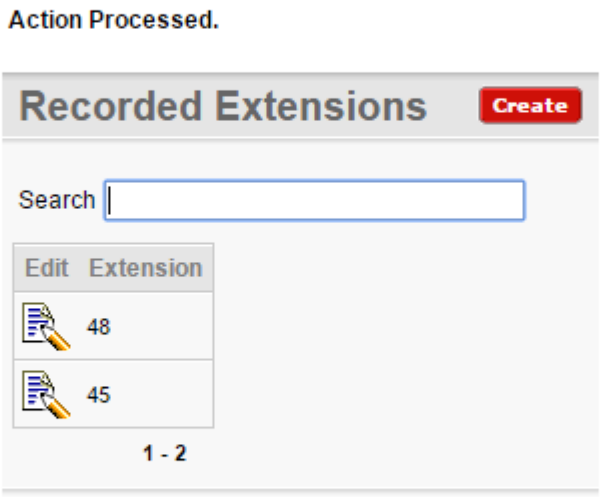
2. Enter the extension number (DN) of the phone and click the **Create** Button.



Edit Recorded Extension

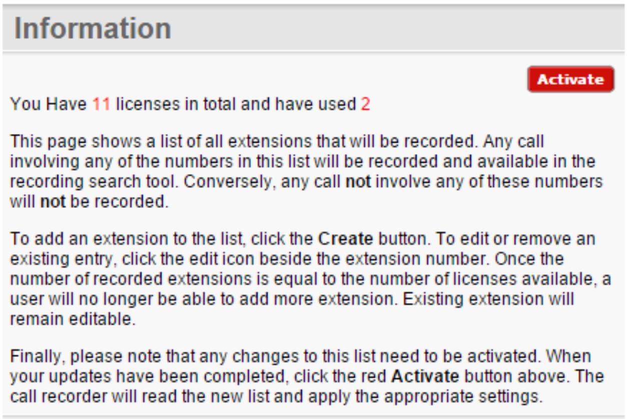
Extension 48

This phone will now appear in the list.



Action Processed.

3. You may continue to add or edit phones in the list within your license limit. Once you reach the limit, the Create button becomes inactive.
4. To start recordings for the updated list, click the **Activate** button



You Have 11 licenses in total and have used 2

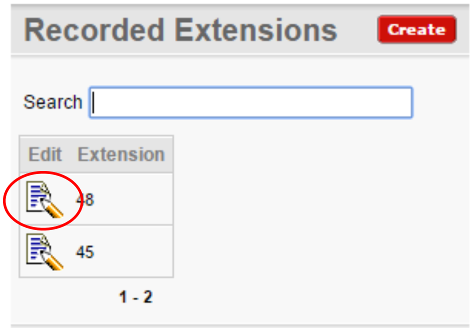
This page shows a list of all extensions that will be recorded. Any call involving any of the numbers in this list will be recorded and available in the recording search tool. Conversely, any call **not** involve any of these numbers will **not** be recorded.

To add an extension to the list, click the **Create** button. To edit or remove an existing entry, click the edit icon beside the extension number. Once the number of recorded extensions is equal to the number of licenses available, a user will no longer be able to add more extension. Existing extension will remain editable.

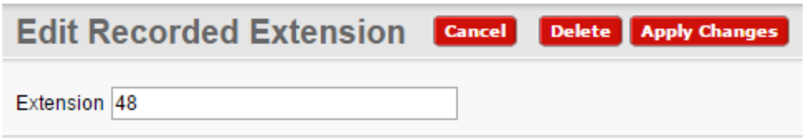
Finally, please note that any changes to this list need to be activated. When your updates have been completed, click the red **Activate** button above. The call recorder will read the new list and apply the appropriate settings.

To change or delete a phone from the recording list:

1. From the main **Manage Recorded Extensions** page, click the **edit** icon next to the extension



2. Edit the extension number (DN) to change it and click the **Apply Changes** button, or press the **Delete** button to remove the extension from the list.



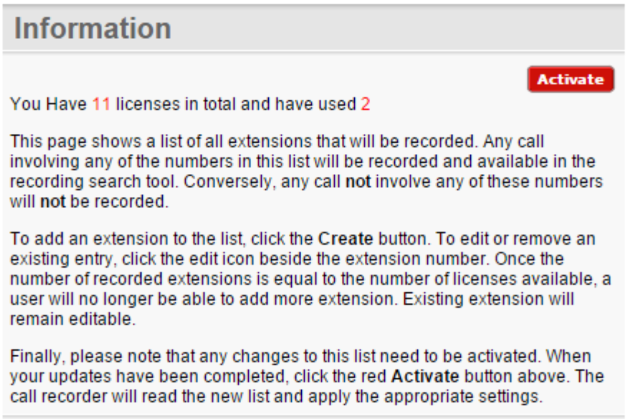
Edit Recorded Extension

Extension 48

The list will be updated.

3. Continue making changes within your license limit.

4. To start recordings for the updated list, click the **Activate** button



Information

You Have 11 licenses in total and have used 2

This page shows a list of all extensions that will be recorded. Any call involving any of the numbers in this list will be recorded and available in the recording search tool. Conversely, any call **not** involve any of these numbers will **not** be recorded.

To add an extension to the list, click the **Create** button. To edit or remove an existing entry, click the edit icon beside the extension number. Once the number of recorded extensions is equal to the number of licenses available, a user will no longer be able to add more extension. Existing extension will remain editable.

Finally, please note that any changes to this list need to be activated. When your updates have been completed, click the red **Activate** button above. The call recorder will read the new list and apply the appropriate settings.

9.3. Additional user accounts

FTR users have access to the recording application page that allows recordings to be browsed, searched and retrieved.

To become an FTR user, you must be a member of the ATEA_FTR_User group on the CUCM. An FTR administrator will then assign which recording groups you have access to.

10.Troubleshooting

Troubleshooting tips and setup tasks.

Issue	Tip
Some recordings are not displaying on the recording page	Possible issues: 1. The date range is incorrect. 2. The recording has not been processed yet. It may take up to ten minutes for a recording to display on-screen 3. There may be an issue with recordings not being captured. a. Check the Linux directory /var/recordings/ to see if the recording files are present. b. Check the directory numbers for the caller and calling party. If this is a five or six digit number that is high, contact Atea Support regarding a possible UDP port number issue.
A specific phone is not being recorded	Possible issues: 1. The phone must have the recording profile set up in the CUCM 2. The phone number (DN) must be included in the license list.
Recording files are of zero duration	Possible issues: Wrong voice codec / not enough resources FTR Solutions using G.711 only 1. On the UCM, check that the calls are set for G.711 2. If UCM transcoding is used to convert calls to G.711, check there are sufficient transcoding resources. Note: FTR does not record G.722 calls FTR solutions using g.729 option 1. Check that G.729 option is enabled 2. Check that the G.729 license file is present 3. Check that there are sufficient G.729 licenses installed (Atea) Blocked access 1. A firewall is blocking the access to the SIP trunk or to the disk with the recordings. This is a configuration issue that sometimes occurs during initial commissioning.
Recordings display as “not found” on the recording display screen	The recording file may have been moved or archived from the disk. Restore the file to the original location. Alternatively, search for the file name in the location where the recording files have been moved or archived to.
Recording disk space is full / exceeds capacity threshold	Move or archive some recording files.
Oracle database is full / approaching full	Contact Atea support to arrange purging of selected database records

Issue	Tip
Recordings are cut off after 16 minutes	Adjust the “SIP Session Expires Timer” to the value 86400 (which is 24 hours in seconds). The default setting for this means recording automatically ends at 16 minutes, as the RFC4028 re-invite is not used. This timer is a system setting under: Cisco CallManager (Active) > System > Service Parameter Configuration > SIP Session Expires Timer
Some recordings overlap falsely when using G.729 codec	Silence suppression for G.729 needs to be disabled. On the CallManager, set the parameter **Strip G.729 Annex B (Silence Suppression) from Capabilities** to **True**.