telisca

Administrator’s Guide

telisca Recording

Directory
Phone Directory
Jabber UDS Server
Web Directory
IPS Popup / Reverse Lookup
Personal Directory
H350 Video Conf directory
Corporate Speed Dials
ClickNDial
Alerting
Voice Alert
IPS Pager
Admin tools
Morning Check
Phone Remote
Phone Robot
Provisioning
Phone Deployment
CMS Admin & Selfcare
Extension Mobility Report
Manager Assistant
IP Phone / Jabber Interface

Productivity tools
IPS Phone Config
IPS Alarm Callback
IPS Lock
Wakeup Call
Missed Call Alerter
Conference Center
Busy Alerter Callback
Desktop Popup
Finesse Gadgets
Spark Bot
Attendant Console / IVR / Group
Tannounce
Line Group Manager
Silent Monitoring
Extension Mobility tools
TSSO
Delog / Relog
Pin & Password Manager
Recording
Call Recording
Recording Notification

support@telisca.com
+33 1 4645 0512

1 Overview

telisca Recording solution is a complete recording solution integrating a recording agent and a record management module.

1.1 Integrating recording agent

- Built in Bridge recording.
- CUBE recording.
- Supports G711, G722, G729 CODECs.
- Merge segments and transcode into MP3 audio files.
- Supports calls association (consultation, transfer, conference).
- Fault tolerance configuration.

1.2 Recording management module

- Archive recordings on efficient network storage on predefined time range.
- Encrypt recordings.
- Automatic purge according to defined duration.
- Annotation of recordings with data from corporate/customer directory (AD) or CUCM user/phone data or CSV file.
- User authentication by Active Directory or CUCM User ID.
- Segmentation of authorized users by Windows security groups or CUCM Access Control Groups.
- Web interface to search recordings by last name, first name, location, user id, minimum call duration, beginning time/date range, comments, with contacts segmented and filtered by organization or department.
- Play audio recording streamed via the web interface, with option to download recordings (no plug-in required).
- Reporting of CUCM CDR and archive recordings comparisons.
- Reporting and update of CUCM Recording profile and option.
- Audit of performed listening.
- Add comments to recordings.

Note: The Recording Manager module also support Cisco MediaSense as recording agent.

2 Feature details

2.1 Archiving

Agents record continuously in RAW format, then merged and converted to MP3 on demand.

The recordings are periodically exported by manager on predefined time range, encrypted and stored on network storage on predefined time range (to save bandwidth in rush hour) or on local disk, which may be on separate storage devices as required by the organization of the enterprise. It is possible to define a separate storage device for each cluster as well as per department/company.

2.2 Encryption audio files (optional)

Optionally, it is possible to encrypt the audio files after their export.

2.3 Recordings database

At the same time that the recordings are exported, data furnished by Recording Agent is simultaneously copied and enriched in the database of the telisca Recording application.

The data is complemented by data obtained periodically from the Active Directory/LDAP or CUCM user/phone, also possible to import the data manually or automatically from CSV file.

The information on the caller and the called party is associated with the recording using the telephone number of the caller or the called party. The information stored includes: userID, last name, first name, department, company and location.

2.4 Web interface user authentication

Access to the web interface (HTTPS) for consulting recordings is controlled by authentication based upon the CUCM user or an Active Directory login.

Users authorized to access recordings are defined in the administration, by entity, according to their AD security group or CUCM Access Control Groups.

Authorization and segmentation can be defined in Active Directory or in CUCM. The user may be allowed to listen to his own recordings.

- Active Directory: The supervisor user can be allowed to search and listen for records of agents that have the same attributes (eg Company, Department).
- CUCM: The supervisor user must belong to one or more user groups. The supervisor user will be authorized to search/listen for the records of department/company agents defined and associated with these groups.

2.5 Web user interface search and consulting recordings

Users who are authorized to search recordings for a selected entity may search by:

- user ID,
- last name,

- first name,
- telephone number,
- date / time range,
- call duration.
- comments

The information available in the replicated database is displayed in a search results grid. When the recording may be heard via streaming or commented or, optionally, may be downloaded.

Note: Users can be authorized to search and listen only their owned recordings.

2.6 Database purge

According to retention parameters, database and a physical purge of media files is automatically made, the sessions whose age exceeds the retention limit.

The retention period may be different depending on the department or company of involved participants.

If authorized, the supervisor may mark the recordings from the Web Interface, to select a shorter or longer retention period.

2.7 Provisioning recorded lines

CUCM Recording Profiles and Recording Option can be updated directly from application based on Active Directory attributes defined.

2.8 Reports

- CDR reporting (required manual configuration on Linux platform)

An execution report allows the review of the comparison status of all exports from recording agents and CUCM CDR history data.

- Users and Lines reporting

A report allows the review status and update recording profile and recording option of CUCM.

3 Prerequisites & Architecture Elements

The telisca Recording application is installed on a shared Windows-based or Linux server.

3.1 Recording management module

Supported Servers OS:

- Windows Server 2012 R2 Essentials or Standard
- Windows Server 2016 Essentials or Standard
- Windows Server 2019 Essentials or Standard
- Windows Server 2022 Standard

Application server may be running on virtual machines such as:

- VMWare ESX,
- Hyper V
- Cisco UCS, UCS-E

Minimum hardware configuration needed by application:

- CPU: 1 vCPU
- RAM: 6GB
- Disk: 100GB (may vary if database and recording files are stored locally)

Prerequisites OS features:

- .NET 4.8

Strongly recommended OS parameters:

- NTP Server for time synchronization
- Server name should be resolved by DNS

3.2 Recording agent module (in case of separate server installation)

Supported Servers OS:

- Windows Server 2012 R2 Essentials or Standard
- Windows Server 2016 Essentials or Standard
- Windows Server 2019 Essentials or Standard
- Windows Server 2022 Standard

- Ubuntu 20.04 LTS

Application server may be running on virtual machines such as:

- VMWare ESX,
- Hyper V
- Cisco UCS, UCS-E

Minimum hardware configuration needed by application:

- CPU: 1 vCPU
- RAM: 4GB
- Disk: 40GB

Strongly recommended OS parameters:

- NTP Server for time synchronization
- Server name should be resolved by DNS

3.3 Database

Database, used to store registered call information and user's information associated, can be installed on same server as application or on another server.

Internal database (PostgreSQL) can be installed and configured during installation process.

External database can be configured (on the same server or remotely), following versions of database servers are supported:

- Microsoft SQL Server 2008 R2 +
- PostgreSQL 9.4+

Database disk size can be up to several GB depending of number of recorded calls and retention period.

3.4 Cisco Unified Communications Manager

Cisco Unified Communications Manager are supported from version 9.1. On CUCM, AXL SOAP API is used to read directory and may be used to populate directory number recording profile.

A CUCM Application User needs to be created, with AXL SOAP read rights. In case of provisioning recorded lines, AXL Write access is also required.

3.5 LDAP/AD server

LDAP/AD server can be used to authenticate and/or authorize users or may be used to populate users directory number database. An application user is needed with read rights.

3.6 Cisco MediaSense

Cisco MediaSense servers (version 9 and upper) are also supported as recording agent.

3.7 Recording file storage

Recording are exported from recording agents mp3 format, in mp4 format from MediaSense, and optionally encrypted.

They can be stored on recording manager server or on shared on the LAN. Recording server uses SMB/CIFS connections to mount network drive from storage servers.

Disk must be correctly sized to be able to store registered call during retention period. To calculate disk size, take into account the following consideration: the amount of storage space required depends on a number of factors, such as the number of calls recorded, the duration, duty cycle and the retention period desired.

According to Cisco, files in .mp4 format average about 18 MB/hour for dual-channel audio. According to our tests, files in mp3 format require a similar size.

3.8 Cisco Unified Communications Manager CDR

Optionally Recording manager can check the CUCM Call Detail Record to compare it for recorded lines with the recorded calls exported. In this case, billing server have to be configured on CUCM and needs to be available on CUCM (CUCM has limit of 3 billing servers).

Note: Requires a manual configuration on Linux platform.

3.9 Web UI browser support

• Internet Explorer	9.0+
• Chrome	3.0+
• Firefox	21+

3.10 Network flow requirements

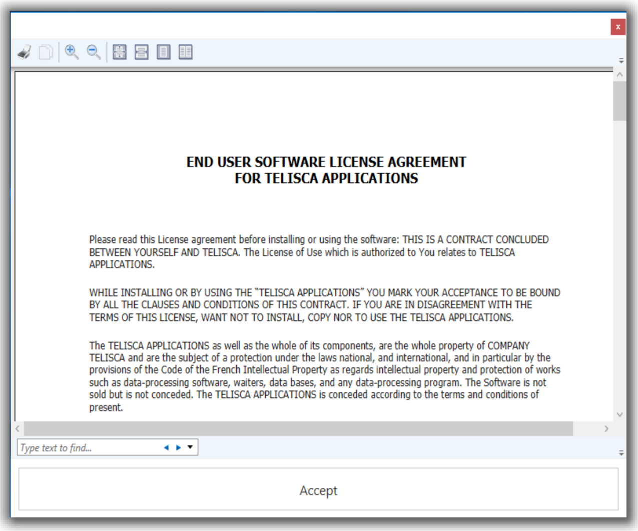
Source	Destination	Protocols/ports
Recording Manager server	CUCM (AXL SOAP)	HTTPS 8443
CUCM CDR (optional)	Recording Manager server	SFTP 22
Recording Manager server	AD/LDAP server	tcp 389 (may be changed)
Recording Manager server	Recording Agent (optional)	REST HTTPS 8440 (may be changed)
Recording Manager server	MediaSense pub/sup (optional)	REST HTTPS 8440
CUCM	Recording Agents	SIP tcp 5060 (may be changed)
IP Phones (Built in Bridge)	Recording Agents	RTP udp 16384 – 32767 (may be changed)
CUBE	Recording Agents	SIP tcp 5060 (may be changed)
CUBE	Recording Agents	RTP udp 16384 – 32767 (may be changed)
Recording Manager server	File Server (optional)	SMB/CIFS tcp 139, 445; udp 137, 138
Recording Manager server	Database PostgreSQL (optional)	tcp 5432 (may be changed)
Recording Manager server	Database MSSQL (optional)	tcp 1433
Web UI Client	Recording Manager server	HTTPS 8445 (may be changed)

4 Installation

4.1 Windows Server installation

telisca Recording Manager

intelligent indexing and powerful search/playback recording solution

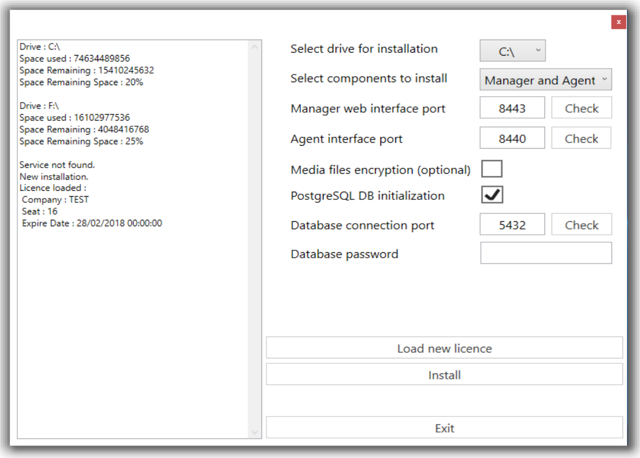


END USER SOFTWARE LICENSE AGREEMENT
FOR TELISCA APPLICATIONS

Please read this License agreement before installing or using the software: THIS IS A CONTRACT CONCLUDED BETWEEN YOURSELF AND TELISCA. The License of Use which is authorized to You relates to TELISCA APPLICATIONS.

WHILE INSTALLING OR BY USING THE "TELISCA APPLICATIONS" YOU MARK YOUR ACCEPTANCE TO BE BOUND BY ALL THE CLAUSES AND CONDITIONS OF THIS CONTRACT. IF YOU ARE IN DISAGREEMENT WITH THE TERMS OF THIS LICENSE, WANT NOT TO INSTALL, COPY NOR TO USE THE TELISCA APPLICATIONS.

The TELISCA APPLICATIONS as well as the whole of its components, are the whole property of COMPANY TELISCA and are the subject of a protection under the laws national, and international, and in particular by the provisions of the Code of the French Intellectual Property as regards intellectual property and protection of works such as data-processing software, waiters, data bases, and any data-processing program. The Software is not sold but is not conceded. The TELISCA APPLICATIONS is conceded according to the terms and conditions of present.



```
Drive : C:\
Space used : 74634489856
Space Remaining : 15410245632
Space Remaining Space : 20%

Drive : F:\
Space used : 16102977536
Space Remaining : 4048416768
Space Remaining Space : 25%

Service not found.
New installation.
Licence loaded :
 Company : TEST
 Seat : 16
 Expire Date : 28/02/2018 00:00:00
```

Select drive for installation	C:\	
Select components to install	Manager and Agent	
Manager web interface port	8443	Check
Agent interface port	8440	Check
Media files encryption (optional)	☐	
PostgreSQL DB initialization	☑	
Database connection port	5432	Check
Database password		

A setup program allows an automatic installation of telisca Recording Agent, telisca Recording Manager and PostgreSQL database. To run, it requires .Net 4.5.x to be installed.

Please launch program: TRM_Setup.exe and read and accept the Software license agreement, by clicking on the Accept button.

Select the drive to install the application. At least 100GB of disk needs to be available. If two disks have been created, C: is generally dedicated to the Windows System and D: to the application.

By default the setup install Manager and Agent components. You can select only Manager or Agent component to setup.

The default port to access to telisca Recording Manager is 8445 and Agent API port is 8440. You may check port availability by Check button. It can be modified later if required by the setup program.

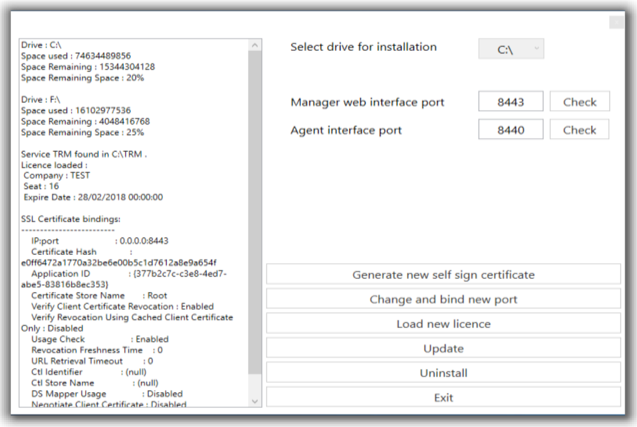
Select if you want the media files to be encrypted. You cannot change this setting afterward.

In case of internal DB initialization, you can change default database port and password for database connection with login 'trm'. Please save this password if you want to connect directly to PostgreSQL pgAdmin administration interface.

In order to install, the application you need to load a Recording license file. It is an XML file with name MSENSE_lic.xml. It includes the name of the Company, the number of simultaneous recording, the duration (generally unlimited).

Then click on Install. During installation, if program detect presents of old version data, the data will be backup and zipped in TRM/BACKUP folder of selected drive.

Then installation is complied, for initial configuration, you can connect telisca Recording Manager administration by https://localhost:8445 using login 'config' with empty password (this login can be used only locally on the server).



```
Drive : C:\
Space used : 74634489856
Space Remaining : 15344304128
Space Remaining Space : 20%

Drive : F:\
Space used : 16102977536
Space Remaining : 4048416768
Space Remaining Space : 25%

Service TRM found in C:\TRM .
Licence loaded :
 Company : TEST
 Seat : 16
 Expire Date : 28/02/2018 00:00:00

SSL Certificate bindings:
-------------------------
   IP:port                   : 0.0.0.0:8443
   Certificate Hash          :
e0ff6472a1770a32be6e00b5c1d7612a8e9a654f
   Application ID            : {377b2c7c-c3e8-4ed7-
abe5-83816b8ec353}
   Certificate Store Name       : Root
   Verify Client Certificate Revocation : Enabled
   Verify Revocation Using Cached Client Certificate
Only : Disabled
   Usage Check                  : Enabled
   Revocation Freshness Time    : 0
   URL Retrieval Timeout        : 0
   Ctl Identifier               : (null)
   Ctl Store Name               : (null)
   DS Mapper Usage              : Disabled
   Negotiate Client Certificate : Disabled
```

Select drive for installation: C:\

Manager web interface port: 8443

Agent interface port: 8440

After installing, or when launching again the setup when the application is installed, we get this screen.

If self-sign certificate accidentally deleted or expired, it is possible to generate new one clicking on 'Generate new self-sign certificate'.

It is possible to change the Web https port used to access telisca Recording Manager Web interface by entering a new https port value and clicking on 'Change and bind new port'.

Also, it is possible to upgrade the license file (to replace an evaluation license or for additional licenses).

To install a new version, click on Update, the previos version data will be backup and zipped in TRM/BACKUP folder of selected drive, actually only manual rollback is possible by unzip and overwrite backup to application folder. During rollback process the application services must be stoped.

To uninstall, the application (telisca Recording Agent, telisca Recording Manager, PostgreSQL for TRM), click on Uninstall.

4.2 Linux Server installation

Currently, Linux Server installation can be done by telisca staff.

4.3 External database Server

Internal database (PostgreSQL) is installed and configured during installation process.

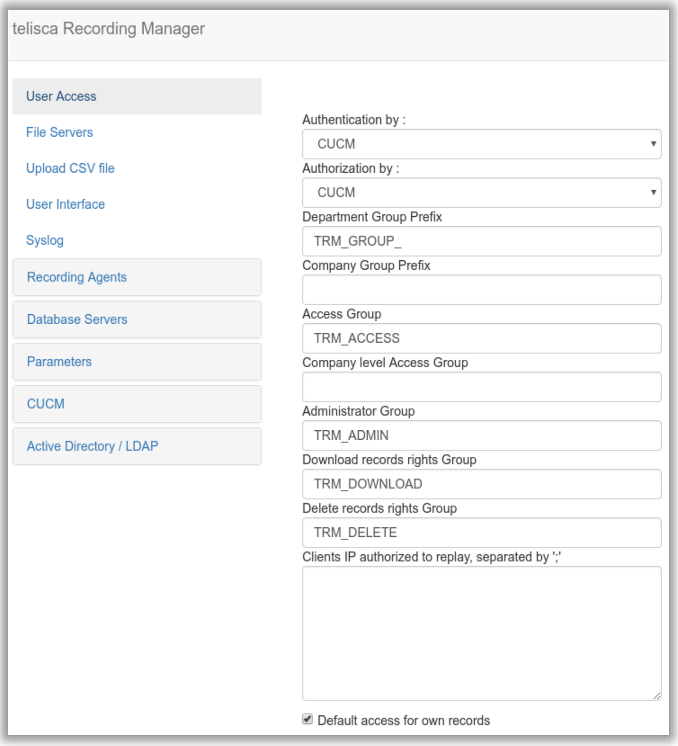
External database can be configured (on the same server or remotely), SQL DDL scripts (for PostgreSQL and Microsoft SQL Server) can be found in installation package in **DATA\SQL SCRIPT** directory.

The database login set is 'trm'. The password 'PasswordToChange!' property in files, needs to be changed before executing the scripts.

5 Settings

This chapter describes the settings that are available from telisca Recording Manager Settings menu.

5.1 User Access



Authentication by : CUCM
Authorization by : CUCM
Department Group Prefix: TRM_GROUP_
Company Group Prefix:
Access Group: TRM_ACCESS
Company level Access Group:
Administrator Group: TRM_ADMIN
Download records rights Group: TRM_DOWNLOAD
Delete records rights Group: TRM_DELETE
Clients IP authorized to replay, separated by ';':
☑ Default access for own records

Telisca Recording can check authentication (login / password) and authorization (user's rights) both from Active Directory / LDAP or CUCM or a mix. This take advantage of Active Directory / LDAP security groups or CUCM Access Control Groups.

If 'Active Directory / LDAP' is used for authentication or authorization, the menu items 'Server' and 'Fields' in 'Active Directory / LDAP' have to set.

If CUCM is used for authentication or authorization, at least one server in menu item 'Server' in 'CUCM' have to set.

In case of a mix authentication/authorization is used you need to define which Active Directory / LDAP attributes contains the CUCM UserId in 'AD attribute to match CUCM UserId' field.

5.1.1 Active Directory / LDAP authorization

The Active Directory / LDAP user which is in security group in field 'Access Group' will be authorized to search, play and comment the recordings limited by user's department field in application user's data associated with recordings. If the user is in the security group specified in 'Company level Access Group' the access to recordings is limited depending of user's company field instead of department field.

The users which is in the security group specified in 'Download Group' is authorized to download an mp3 file containing the recording.

The user which is in the security group 'Administrator Group' is authorized to view and update the administrator's settings and has a full access to all of the recordings.

5.1.2 CUCM authorization

In order to use the CUCM authorization you need to define Access Control Groups for user Search and play right in field 'Access Group', mp3 download right in 'Download Group' field and administrator's right in 'Administrator Group' field.

Additionally, you need to create on CUCM Access Control Groups with the define prefix in 'Department Group Prefix' for each department to search or 'Company Group Prefix' for companies, if the user is part of Access Control Groups specified in 'Company level Access Group' field. The value of Department Group Prefix does not need to be included as part of Company Group Prefix.

All non-alphanumeric characters in department and company names will be replaced by dash (-), while creating in CUCM.

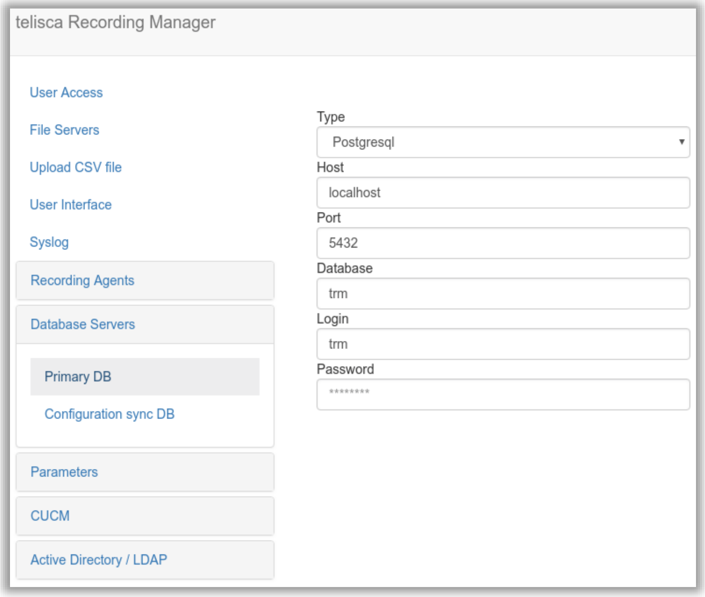
In case of Active Directory / LDAP user data update source, the option 'Replace by '-' all non-alphanumeric characters in department and company values' in 'Fields' in 'Active Directory / LDAP' menu item has to be checked.

5.1.3 Additional authorization options

Option 'Default access for own records' may be checked to allow the users search, play and comment only own records of the user, based on user's phone number. If option 'Default access for own records' is checked, security groups or CUCM access control groups configuration not required to have access to own records.

For all the above settings, except administrator access, there is also a check on the IP address of the workstation that are authorized to connect to Telisca Recording, if the 'Clients IP authorized to replay, separated by ';'' field is not empty.

5.2 Database Server



Type: Postgresql
Host: localhost
Port: 5432
Database: trm
Login: trm
Password: ********

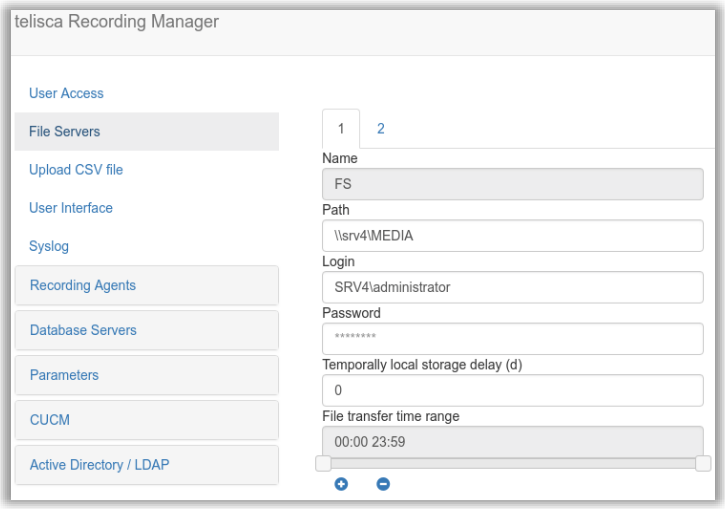
Internal database (PostgreSQL) can be installed and configured during installation process. External database can be configured (on the same server or remotely), SQL DDL scripts can be found in installation package, following type of database servers are supported:

- Microsoft SQL Server
- PostgreSQL

To configure the database, select the 'Type' and enter the following information Host, Port (in case Microsoft SQL Server the port can be empty if default 1433 is used), Database name, Login and Password.

The configuration can be checked clicking on check button. All the modifications have to be saved by clicking save button.

5.3 File Servers



Name: FS

Path: \\srv4\MEDIA

Login: SRV4\administrator

Password: ********

Temporally local storage delay (d): 0

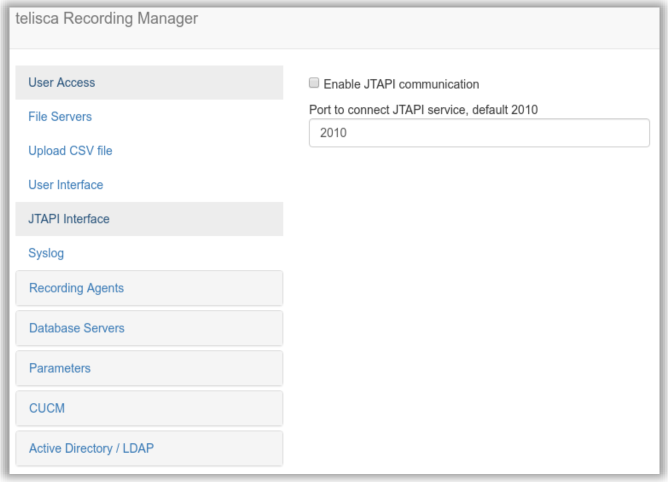
File transfer time range: 00:00 23:59

The recording manager application supports multi remote file server's configurations. To add a new file server, click on the plus icon. It is also possible to delete selected file server clicking minus button. The configuration can be tested by clicking on check button.

The following information are required per server:

- Name: internal name, must be unique.
- Path: UNC path (ex: \\server\share);
- Login: User to connect remote server (ex: domain\user or server\user).
- Password: User password.
- Temporally local storage delay (d): Temporally local storage delay of media files before transferring to the file server, default 0 days.
- File transfer time range: Media files transfer time range to the file server, default is no limitation. This is useful to save network bandwidth during working hours between remote sites.

5.4 JTAPI interface



☐ Enable JTAPI communication

Port to connect JTAPI service, default 2010: 2010

The recording manager application supports socket communication with telisca CTI application (installed by telisca Global setup).

It is used in Selective Recording mode, to start/stop the recording from the Finesse Gadget, IP Phone Service or Attendant Console.

5.5 Recording Agents (MediaSense or telisca Recording Agent)

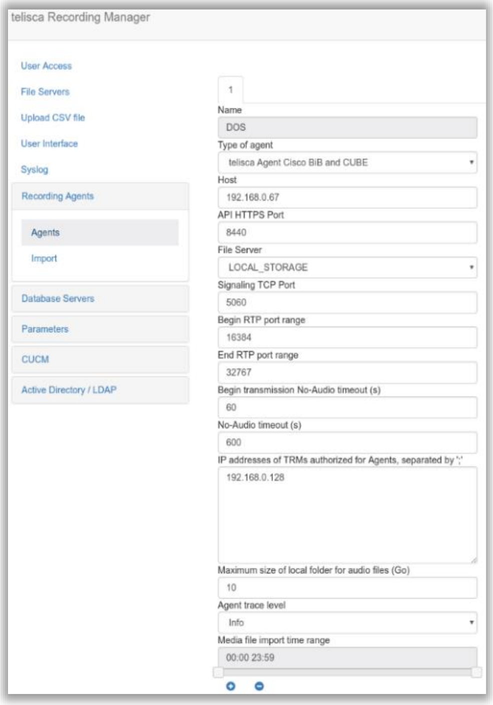
5.5.1 Agents

The recording manager application supports multi-agents' configuration and different type of recording agents: telisca Agent (Cisco Bultin-Bridge and CUBE) or Cisco MediaSense.

To configure a new agent, click on the plus icon. It is also possible to delete the selected agent clicking minus button. The configuration can be tested by clicking on check button. All the modifications have to be saved by clicking save button.

Agent type 'telisca Agent Cisco Bultin-Bridge and CUBE' requires the following information:

- Name: internal name, must be unique.
- Host: IP address or DNS of agent host.
- Https Port : Agent API Https Port, default port is 8440.
- File Server: List of internal local storage or external file servers' resources, as configured in the application, default is local storage.
- Signaling TCP Port: SIP trunk signaling port, default is 5060.
- Begin RTP port range: First UDP port of the RTP range, default is 16384.
- End RTP port range: Last UDP port of the RTP range, default is 32767.



Name: DOS

Type of agent: telisca Agent Cisco BiB and CUBE

Host: 192.168.0.67

API HTTPS Port: 8440

File Server: LOCAL_STORAGE

Signaling TCP Port: 5060

Begin RTP port range: 16384

End RTP port range: 32767

Begin transmission No-Audio timeout (s): 60

No-Audio timeout (s): 600

IP addresses of TRMs authorized for Agents, separated by ';': 192.168.0.128

Maximum size of local folder for audio files (Go): 10

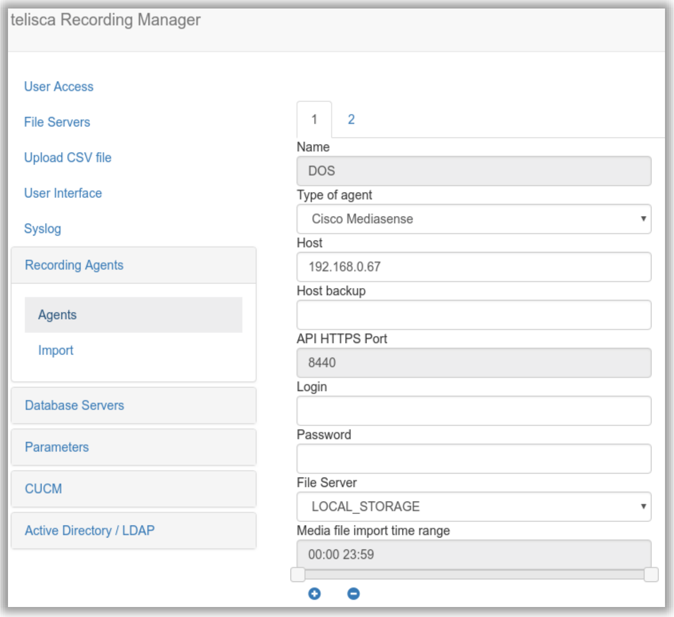
Agent trace level: Info

Media file import time range: 00:00 23:59

- Begin transmission No-Audio timeout: No RTP timeout of beginning of the SIP call, default is 60 seconds. During this time application will wait RTP stream for the answered call, then the call will be closed wit error flag.
- No-Audio timeout: No RTP timeout during the SIP call, default is 600 seconds. During this time application will wait RTP stream during the call, then the call will be closed wit error flag.
- IP addresses of Recording Manager's authorized for Agents, separated by ';' : Agents accepts HTTPS requests only from the list, default is local Recording Manager's IPv4 address.
- Maximum size of local folder for audio files (Go): Temporary agent storage, default is 10 Go. Storage must be correctly sized to be able to store registered calls before been imported to Recording Manager. The size should take into account: the number of calls per hour, average call length, CODEC used, import time range, potential Recording Manager down time and import period.
- Recording Agent log's level: Can be 'disabled', 'forced', 'error', 'treatment', 'methods', 'maximum', default is 'methods'.
- Media file import time range: Import from Agent time range, default is no limitation. It may be useful to define a time range when the Recording Agent and Recording Manager are not on the same server, to limit the use of bandwidth between working hours. The size allowed to the Recording Agent should be then increased to store one day of recording.

Internal Agent type 'telisca Agent Cisco BiB and CUBE' can be installed and configured during

Agent type 'MediaSense' required the following information:



Name: DOS

Type of agent: Cisco Mediasense

Host: 192.168.0.67

Host backup:

API HTTPS Port: 8440

Login:

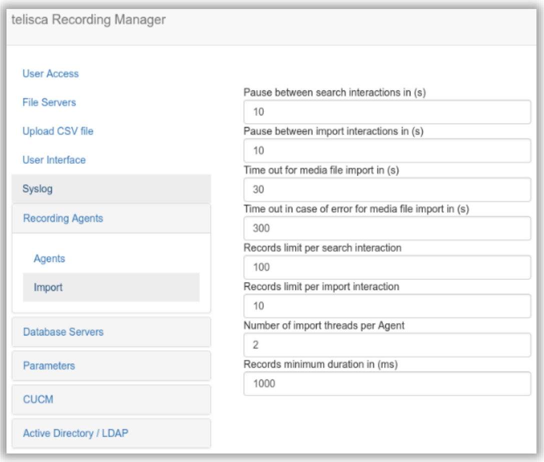
Password:

File Server: LOCAL_STORAGE

Media file import time range: 00:00 23:59

- Name : internal name, must be unique.
- Host : IP address or DNS of MediaSense primary host.
- Host backup : IP address or DNS of MediaSense backup host (optional).
- Login : UserId of CUCM End user associated with MediaSense.
- Password : Password of CUCM End user associated with MediaSense.
- File Server : List of internal local storage or external file servers, configured on the application, default is local storage.
- Media file import time range : Import from Agent time range, default is no limitation.

5.5.2 Import



Pause between search interactions in (s): 10

Pause between import interactions in (s): 10

Time out for media file import in (s): 30

Time out in case of error for media file import in (s): 300

Records limit per search interaction: 100

Records limit per import interaction: 10

Number of import threads per Agent: 2

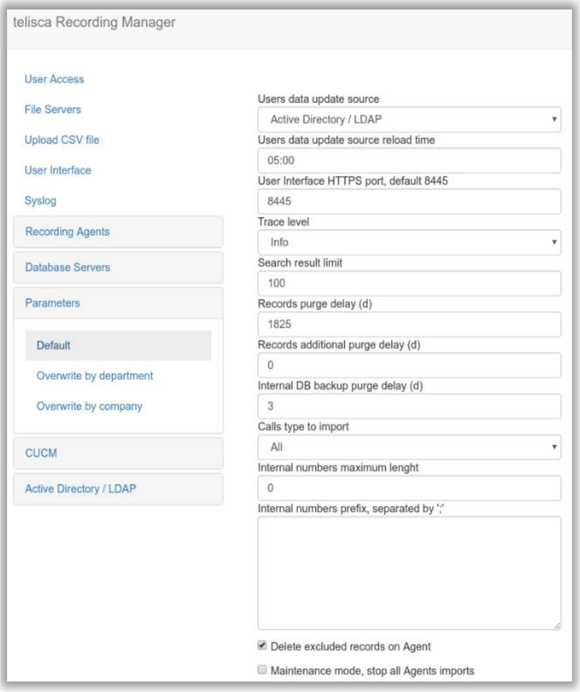
Records minimum duration in (ms): 1000

The recording manager uses these parameters to import the recordings from agents. The imports parameters applied on all agents. These are advanced parameters, do not change them unless requested by telisca Support. All the modifications have to be saved by clicking save button.

- Pause between search interactions in (s) : Pause between requests from recording manager to agents to get the list of session to import, default is 10 seconds.
- Pause between import interactions in (s) : Pause per thread between requests from recording manager to agents to import media, default is 10 seconds.
- Time out for media file import in (s) : default is 30 seconds. It is the maximum time to import a recording from the agent. It takes into account the merge/media conversion.
- Time out in case of error for media file import in (s) : Default is 300 seconds.
- Records limit per search interaction : Default is 100 records.
- Records limit per import interaction : default is 10 records. Each time the Manager requests the agent to import recordings, only this number of session will be exported per interaction.
- Number of import threads per Agent : default is 2 threads.
- Records minimum duration in (ms) : default is 1000 milliseconds. This is the minimum duration of a recording session that is imported in telisca Recording Manager.

5.6 Parameters

5.6.1 Default



Users data update source: Active Directory / LDAP

Users data update source reload time: 05:00

User Interface HTTPS port, default 8445: 8445

Trace level: Info

Search result limit: 100

Records purge delay (d): 1825

Records additional purge delay (d): 0

Internal DB backup purge delay (d): 3

Calls type to import: All

Internal numbers maximum lenght: 0

Internal numbers prefix, separated by ';':

☑ Delete excluded records on Agent

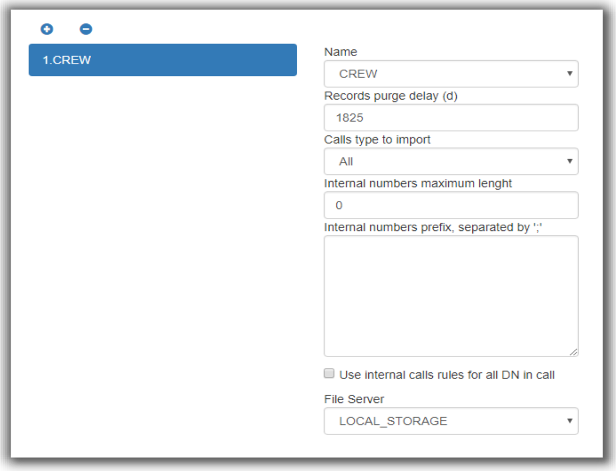
☐ Maintenance mode, stop all Agents imports

The following parameters may be changed. All the modifications have to be saved by clicking on the save button.

- Users data update source: Directory users data source, can be 'Active Directory / LDAP' , 'CUCM' or no source. In case of 'Active Directory / LDAP' is used the menu items 'Server' and 'Fields' in 'Active Directory / LDAP' have to set. If CUCM is used at least one server in menu item 'Server' in 'CUCM' have to set. Default is no source set.
- Users data update source reload time: Time to reload configured user data source. Default is not set.
- HTTPS port, default 8445: Web user interface HTTPS port. If amended, requires telisca Recording Manager service to be restarted.
- Recording Manager's log level: Can be 'disabled', 'forced', 'error', 'treatment', 'methods', 'maximum', default is 'methods'.
- Search result limit: Maximum number of recordings displayed on search. Default is 100 records.
- Records purge delay (d): Recording media purge delay (retention period) in days, applied by default. Default value is 1825 days (5 years).
- Records additional purge delay (d): If set the user can extend the retention period from the Web User Interface for a selected recording, adding the configured value in days, default is 0 (not set).
- Internal DB backup purge delay (d): If the internal database is configured. The application does a backup every midnight and keeps the backups for a defined period in days, default is 3 days.
- Call type: Default calls type import filter, can be 'Internal Only',' External Only', 'All', default is 'All' calls.
- Internal numbers maximum length: Required if calls type import filter set to 'Internal Only' or 'External Only', default is 0 (not set)
- Internal numbers prefixes, separated by ';': Can be set if internal and external numbers have same length, default is empty.
- Delete excluded records on Agent: Can be checked to delete all excluded records on Agent side, default is unchecked.
- Maintenance mode, stop all Agents imports: Stop all imports from all of the Agents and DB data modification if checked, default is unchecked.
- Password for media file encryption: Media files encryption password, if password is set the field will be not visible anymore, default is empty.

Please save the password on a secured media. If a complete reinstall would be required, it would not be possible to un-encrypt the recordings without this password. Password cannot be changed if set.

5.6.2 Overwrite by department / company



Name: CREW

Records purge delay (d): 1825

Calls type to import: All

Internal numbers maximum lenght: 0

Internal numbers prefix, separated by ';'

□ Use internal calls rules for all DN in call

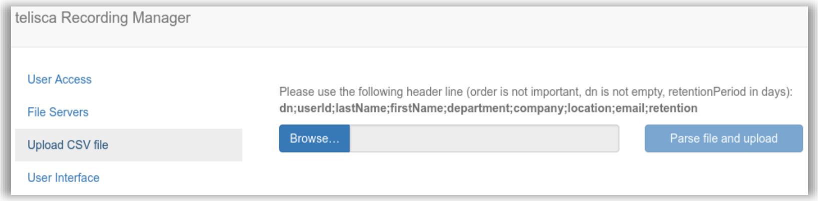
File Server: LOCAL_STORAGE

The global parameters can be overwritten by department or company configuration. The configuration will be applied if at least one user with the department or company participate the recording.

To add new entity, click on the plus icon, also possible to delete selected entity by minus button. All the modifications have to be saved by save button.

- Name: List of entities available.
- Records purge delay (d): Purge delay to apply, default value 1825 days.
- Call type: Default calls type import filter, can be 'Internal Only', 'External Only', 'All', default is 'All' calls.
- Internal numbers maximum length: Required if calls type import filter set to 'Internal Only' or 'External Only', default is 0 (not set)
- Internal numbers prefix, separated by ';': Can be set if internal and external numbers have same length, default is empty.
- File Server: List of internal local storage or external file servers, configured on the application, default is local storage.
- Use internal calls rules for all DN in call: If checked, new internal calls rules applied to all recording participants, if the user of this entity participate the recording. Default is unchecked.

5.7 Upload CSV file



Please use the following header line (order is not important, dn is not empty, retentionPeriod in days):
dn;userId;lastName;firstName;department;company;location;email;retention

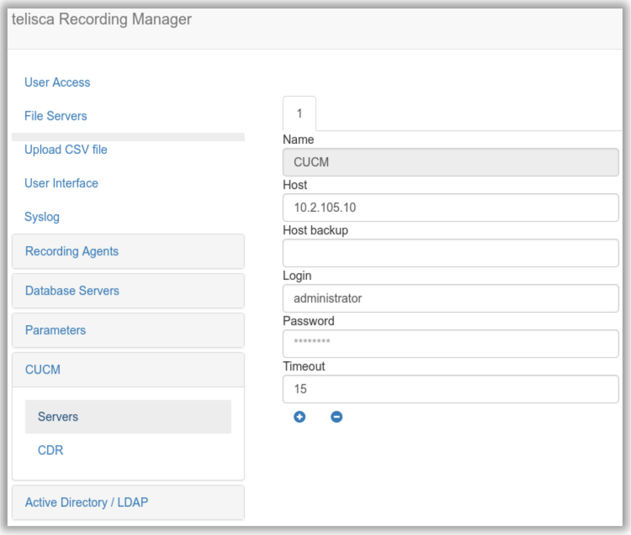
In addition to users data daily auto-update from 'Active Directory / LDAP' or 'CUCM', the data can be updated by CSV file through web UI or the file can copied directly to TRM server (folder CSV of application) .

Use the following header line (columns order is not important, DN must be not empty, retention Period in days): *dn;userId;lastName;firstName;department;company;location;email;retention*

5.8 CUCM

If CUCM is used for authentication or authorization or as users' data source, at least one server in menu item 'Server' in 'CUCM' have to set. All the modifications have to be saved by clicking save button.

5.8.1 Servers



1

Name: CUCM

Host: 10.2.105.10

Host backup:

Login: administrator

Password: ********

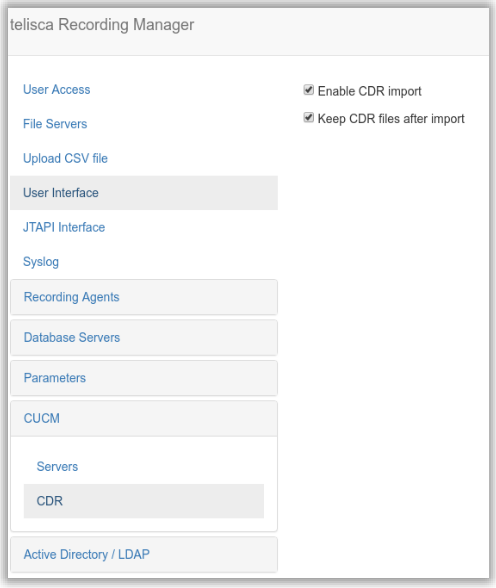
Timeout: 15

The Recording Manager supports multi CUCM configurations. To add an additional CUCM, click on the plus icon. It is also possible to delete selected CUCM, by clicking minus button. The configuration can be tested by clicking on the check button.

The following parameters are required:

- Name: internal name, must be unique.
- Host: IP address or DNS of CUCM publisher host.
- Host backup: IP address or DNS of CUCM subscriber host (optional).
- Login: UserId of CUCM application user, which must be part of AXL SOAP rights group.
- Password: Password of CUCM application user.
- Timeout (s): AXL SOAP requests' timeout, default 15 seconds.

5.8.2 Call Detail Record



☑ Enable CDR import

☑ Keep CDR files after import

The Call Detail Record (CDR) report allows the review of the comparison status of all exports from recording agents and CUCM's CDR history data. All the modifications have to be saved by clicking on the save button. The CDR is uploaded by CUCM on a SFTP Server on telisca Recording Manager's server.

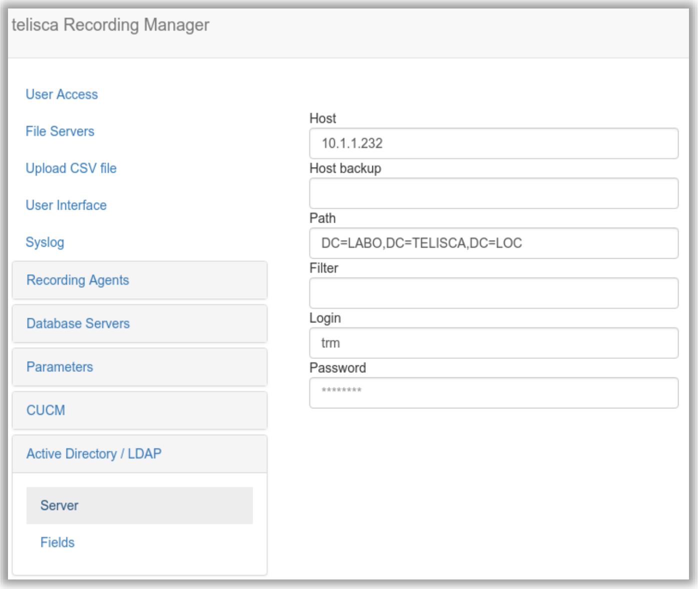
- Enable CDR Report: If checked CDR files import to database.
- Keep CDR files after import: If checked CDR files will be not deleted after import.

If CDR Report is enabled, requires manual setup of SFTP Server, root sftp folder have to set CDR\IN\ folder of TRM.

5.9 Active Directory / LDAP

If 'Active Directory / LDAP' is used for authentication or authorization or as users data source, the menu items 'Server' and 'Fields' in 'Active Directory / LDAP' have to set. The server configuration can be tested by clicking on check button. All the changes have to be saved by clicking save button.

5.9.1 Server



Host: 10.1.1.232

Host backup:

Path: DC=LABO,DC=TELISCA,DC=LOC

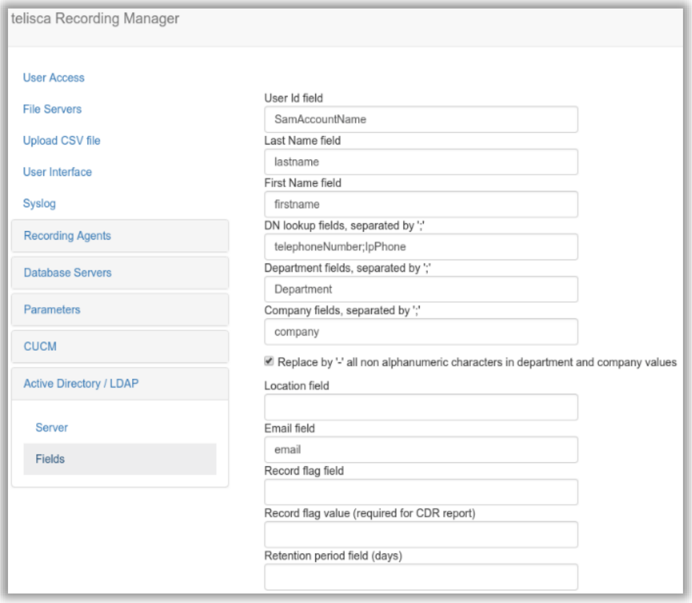
Filter:

Login: trm

Password: ********

- Host: IP address or Active Directory / LDAP host.
- Host backup: IP address or DNS of Active Directory / LDAP backup host (optional).
- Path: AD / LDAP path to search user for authentication or authorization and users data source.
- Filter: AD / LDAP filter to search users for users data source, default is DNs fields is not empty (optional).
- Login: User login to connect AD / LDAP.
- Password: User password to connect AD / LDAP.

5.9.2 Fields



User Id field: SamAccountName

Last Name field: lastname

First Name field: firstname

DN lookup fields, separated by ';': telephoneNumber;IpPhone

Department fields, separated by ';': Department

Company fields, separated by ';': company

☑ Replace by '-' all non alphanumeric characters in department and company values

Location field:

Email field: email

Record flag field:

Record flag value (required for CDR report):

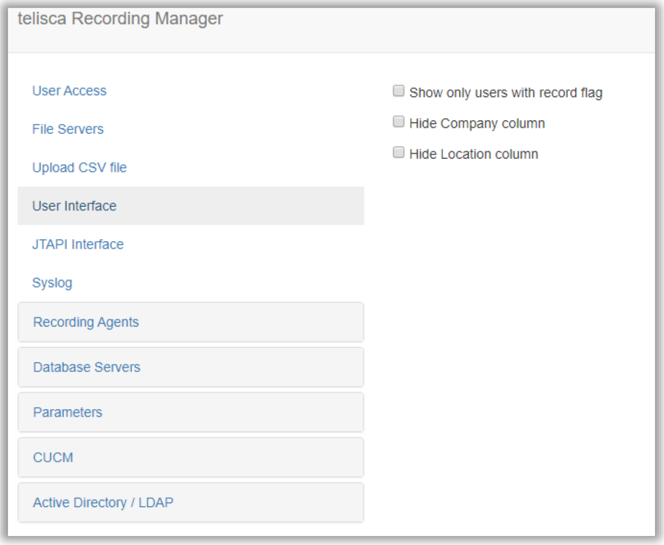
Retention period field (days):

This screen defined which AD/LDAP attributes will be used to enrich the recordings' database with contacts' information.

- User Id field: AD /LDAP User Id field.
- Last Name field: AD /LDAP Last Name field.
- First Name field: AD /LDAP Last Name field.
- DN lookup fields, separated by ';': AD /LDAP DN lookup fields, for each DN new line added to users data.
- Department fields, separated by ';': AD /LDAP Department fields, in case of multiple field the values concatenated.
- Company fields, separated by ';': AD /LDAP Company fields, in case of multiple field the values concatenated.
- Replace by '-' all non-alphanumeric characters in department and company values: Option required in case of a mix authentication/authorization use.
- Location field: AD / LDAP Location field.
- Email field: AD / LDAP Email field.
- Record flag field: AD / LDAP Record flag field for CDR report.

- Record flag value (required for CDR report): Record flag value for CDR report.
- Retention period field (days): AD / LDAP Retention period field per user.

5.10 User Interface



telisca Recording Manager

□ Show only users with record flag

□ Hide Company column

□ Hide Location column

This screen defined end user interface.

- Show only users with record flag: Apply filter on users list on main screen.
- Hide Company column: Hide/Show Company column on main screen.
- Hide Location column: Hide/Show Location column on main screen.

6 CUCM configuration

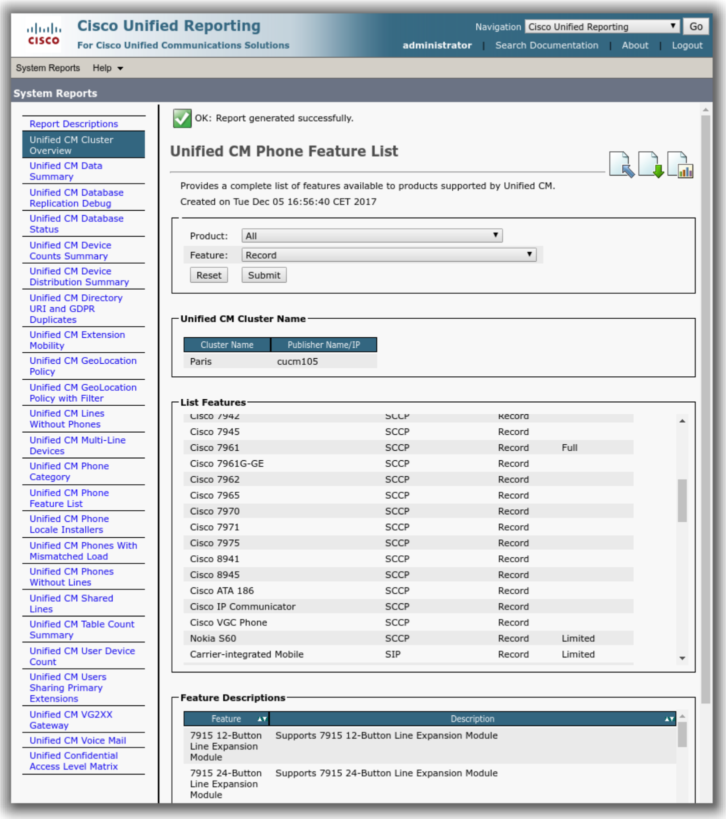
6.1 CUCM configuration for Cisco Built-in-bridge recording

This documentation is inspired from CUCM documentation and describes the required configuration for a recording solution.

6.1.1 Limitations

The following restrictions and limitations exist for monitoring and recording:

Check phones that support Built-in-Bridge recording


Cisco Unified Reporting
For Cisco Unified Communications Solutions
Navigation
Cisco Unified Reporting
Go
administrator
Search Documentation
About
Logout
System Reports
Help
System Reports
Report Descriptions
Unified CM Cluster Overview
Unified CM Data Summary
Unified CM Database Replication Debug
Unified CM Database Status
Unified CM Device Counts Summary
Unified CM Device Distribution Summary
Unified CM Directory URI and GDPR Duplicates
Unified CM Extension Mobility
Unified CM GeoLocation Policy
Unified CM GeoLocation Policy with Filter
Unified CM Lines Without Phones
Unified CM Multi-Line Devices
Unified CM Phone Category
Unified CM Phone Feature List
Unified CM Phone Locale Installers
Unified CM Phones With Mismatched Load
Unified CM Phones Without Lines
Unified CM Shared Lines
Unified CM Table Count Summary
Unified CM User Device Count
Unified CM Users Sharing Primary Extensions
Unified CM VG2XX Gateway
Unified CM Voice Mail
Unified Confidential Access Level Matrix
Reset
Submit

OK: Report generated successfully.

Unified CM Phone Feature List

Provides a complete list of features available to products supported by Unified CM.
Created on Tue Dec 05 16:56:40 CET 2017

Product: All
Feature: Record

Unified CM Cluster Name

Cluster Name	Publisher Name/IP
Paris	cucm105

List Features

Cisco 7942	SCCP	Record	
Cisco 7945	SCCP	Record	
Cisco 7961	SCCP	Record	Full
Cisco 7961G-GE	SCCP	Record	
Cisco 7962	SCCP	Record	
Cisco 7965	SCCP	Record	
Cisco 7970	SCCP	Record	
Cisco 7971	SCCP	Record	
Cisco 7975	SCCP	Record	
Cisco 8941	SCCP	Record	
Cisco 8945	SCCP	Record	
Cisco ATA 186	SCCP	Record	
Cisco IP Communicator	SCCP	Record	
Cisco VGC Phone	SCCP	Record	
Nokia S60	SCCP	Record	Limited
Carrier-integrated Mobile	SIP	Record	Limited

Feature Descriptions

Feature	Description
7915 12-Button Line Expansion Module	Supports 7915 12-Button Line Expansion Module
7915 24-Button Line Expansion Module	Supports 7915 24-Button Line Expansion Module

Connect Cisco Unified Reporting then click System Reports, in the list of reports click the Unified CM Phone Feature List option.

To generate a report of all devices that support recording, choose:

- Product: All
- Feature: Record and click the Submit button.

Codec Consideration During Monitoring or Recording

The codec of the call leg that originates from the IP phone that is being monitored or recorded must remain the same throughout the call.

Security Handling in Monitoring and Recording

Cisco Unified Communications Manager allows a supervisor or administrator to monitor a conversation between an agent and a customer without either party knowing that they are being monitored. For information about using and configuring secure call monitoring and recording, see the "Secure Call Monitoring and Recording" chapter in the Cisco Unified Communications Manager Security Guide.

Intercom

The system does not allow monitoring nor recording of whisper intercom and talkback intercom calls. Configuration of the intercom calling search space (CSS) specifies this limitation.

Recording and Call Hold and Resume

Cisco Unified Communications Manager does not update the recorder when the far-end party puts the call on hold. The recorder will be updated only when a different far-end party resumes the call.

Cisco Unified Communications Manager updates a recorder when the far-end call information changes. The far-end call information contains a call ID, directory number, and device name. If one of these parameters changes, the far-end call information changes.

If a far-end party holds and resumes a call from the same device, Cisco Unified Communications Manager does not update a recorder.

Recording and Call Park and Retrieve

If the far-end party in a remote cluster parks the call, Cisco Unified Communications Manager updates the recorder with an empty far-end party address, provided the remote cluster connects to the local cluster via a SIP trunk or an H323 intercluster trunk. Cisco Unified Communications Manager updates the recorder again when the far-end party retrieves the call either from the same or a difference device. Cisco Unified Communications Manager does not update the recorder if the far-end party that parks the call is in the local cluster. In this case, Cisco Unified Communications Manager only updates the recorder when the call gets retrieved from a different device.

For remote Call Park and Retrieve, the remote Cisco Unified Communications Manager sends the display name Call Park update. This update contains an empty directory number/address; therefore, the far-end address changes to empty. Due to the far-end address change, the local Cisco Unified Communications Manager sends the update with the empty far-end address to the recorder.

In the current Call Park implementation, the far-end or X-Refci may be empty when recording Call Park for Roundtable (RT) phone models such as 997X, 995X and 896X.

Recording and Call Forward No Answer (CFNA)

If the far-end party in a remote cluster blind-transfers the call to a party that has CFNA enabled, Cisco Unified Communications Manager updates the recorder with the ringing party as the far-end party address, provided the remote cluster connects to the local cluster with a SIP trunk or an H.323 intercluster trunk. Cisco Unified Communications Manager updates the recorder again when the call gets forwarded to the CFNA target. Cisco Unified Communications Manager does not update the recorder if the far-end party that blind-transfers g the call is in the local cluster. In this case, Cisco Unified Communications Manager only updates the recorder when the CFNA target answers the call.

When a remote call becomes active, the call state stays active in a local cluster. When a remote far-end party performs a blind call transfer to a new remote far-end party and the party rings, the local Cisco Unified Communications Manager still sees the call state as active. Thus, for remote Call Forward No Answer, the local Cisco Unified Communications Manager sends UPDATE messages to the recorder for a new party because the call state is active.

When a local call becomes active, the call state can change from active to ringing state. The local Cisco Unified Communications Manager can find out a current call state. Thus, for local Call Forward No Answer, the local Cisco Unified Communications Manager sends UPDATE messages to the recorder after a new far-end party answers a call.

Recording and Conference Chaining

If two or more near-end parties are in two or more conferences that are chained together, Cisco Unified Communications Manager can only update the recorder that they are using; separate conferences are identified by the different conference identifiers (b-number). The conference chaining information can be obtained via Call Detailed Records (CDRs).

Cisco Unified Communications Manager sends UPDATE messages to a recorder if the far-end call information changes. For a conference case, the far-end party address specifies the b-number. If the far-end b-number remains unchanged, Cisco Unified Communications Manager does not send the UPDATE messages to the recorder.

Using Route List and/or Multiple Destination Addresses on a SIP Trunk for Multiple Recorders

When using a route list and/or multiple destination addresses on a SIP trunk for multiple recorders, the near-end and far-end recording calls of the same recording session can go to different recorders.

If a Cisco Unified Communications Manager administrator configures a route list with multiple SIP trunks such that each SIP trunk points to a different recorder, Cisco Unified Communications Manager may not send the two recording calls of a recording session to the same SIP trunk, or to the same recorder. Depending on the selection algorithm that is provisioned in the route group, the likelihood of the two recording calls being sent to the same recorder may vary considerably. Similarly, Cisco Unified Communications Manager may not send the two recording calls to the same recorder if the administrator provisioned multiple IP addresses on a SIP trunk such that each IP address points to a different recorder. In this case, the calls get sent to the recorder that is randomly selected from the provisioned IP addresses.

To configure Cisco Unified Communications Manager to support a recorder cluster configuration where a recording session may be redirected to another of the recorders in the cluster, configure a route list or provision multiple destinations on the recording SIP trunk.

6.1.2 Configuration

Turn on IP Phone BIB to Allow Recording

The built-in bridge of the agent phone must be set to On to allow its calls to be monitored or recorded.

You can also set the Built-in Bridge Enable service parameter to On and leave the Built-in Bridge in the Phone Configuration window set to Default.

Use the Device > Phone menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Configure Tones for Monitoring or Recording (Optional)

Set the service parameters for playing tone to True to allow tone to be played either to agent only, to customer only, or to both.

Applications that invoke monitoring or recording can also pass the play tone option to Cisco Unified Communications Manager. The monitoring tone or recording tone plays when either the service parameter or the application specifies the play tone option.

Use the System > Service Parameters menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Enable Recording for a Line Appearance

To enable recording of an agent, set the Recording Option in the line appearance of the agent to one of the following options:

- Automatic Call Recording Enabled
- Selective Call Recording Enabled

Select a pre-created recording profile from the drop-down list box. (Use Device > Device Settings > Recording Profile to configure a recording profile.)

Use the Call Routing > Directory Number menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Add the Record Softkey or Programmable Line Key to the Device Template (Optional)

To enable a user to start and stop recording from a Cisco IP device, add the Record softkey or programmable line key to the device template.

To add the Record softkey, use the Device > Device Settings > Softkey Template menu option in Cisco Unified Communications Manager Administration to create or modify a nonstandard softkey template. Configure the softkey layout for call state connected to have the Record softkey in the selected softkeys list.

To add the Record programmable line key, use the Device > Device Settings > Phone Button Template menu option in Cisco Unified Communications Manager Administration. Enter the button template name, feature, and label.

Create SIP Profile for Recorder

Create a SIP profile for recording. Use the Device > Device Settings > SIP Profile menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

You can check the Deliver Conference Bridge Identifier check box, which delivers additional information (specifically, the b-number that identifies a conference bridge) to the recorder across the SIP trunk. If the check box is left unchecked, the far-end information for the remote conference remains empty.

Check the Deliver Conference Bridge Identifier check box on the remote cluster SIP profile as well.

Note

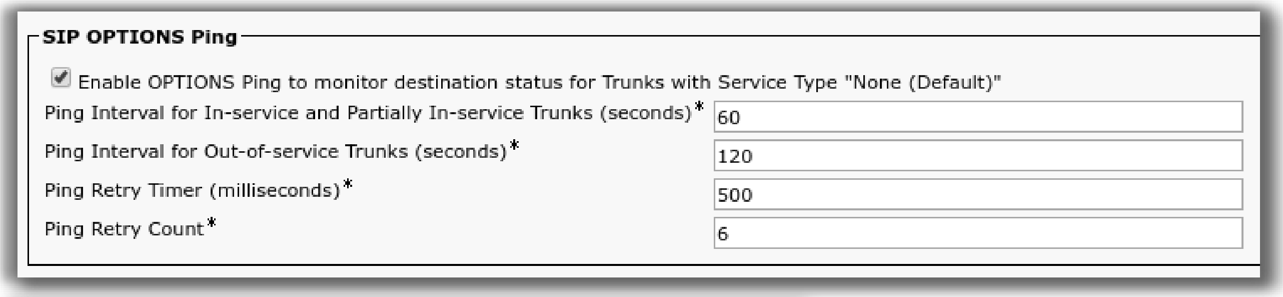
Checking this check box is not required for recording, but the conference bridge identifier helps to update the recorder when recording calls that involve a conference bridge. If you do not create a new SIP profile for recording, you can use the Standard SIP Profile.

See the Cisco Unified Communications Manager Administration Guide for details of configuring SIP profiles.

Configure SIP OPTIONS Ping in SIP Profile.

In multi-agent configuration, recommended to enable SIP Options Ping feature for each recording server. In a single-agent setup, this feature should be disabled .

SIP OPTIONS are requests to the configured destination address on the SIP trunk. If the remote SIP device fails to respond or sends back a SIP error response such as 503 Service Unavailable or 408 Timeout, Cisco Unified Communications Manager tries to reroute the calls by using other trunks or by using a different address.



SIP OPTIONS Ping

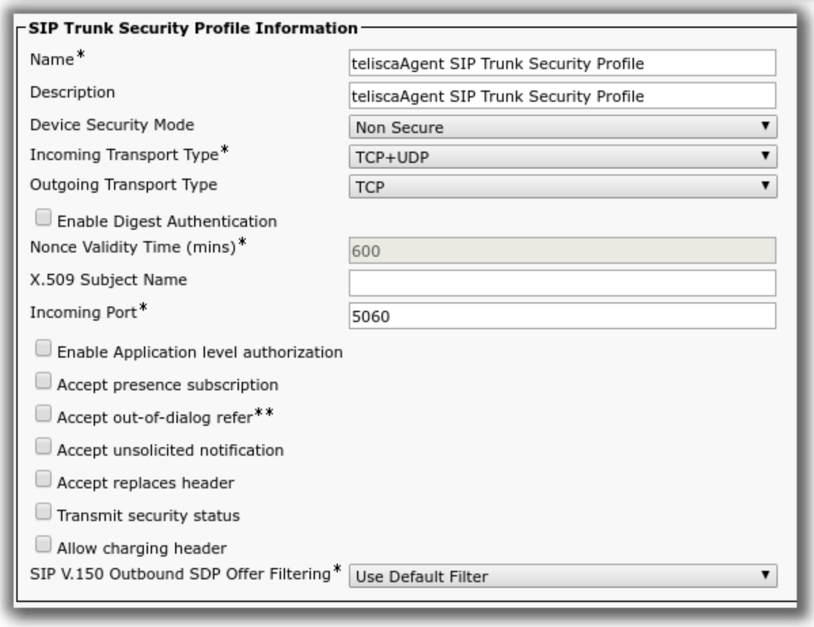
☑ Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)*	60
Ping Interval for Out-of-service Trunks (seconds)*	120
Ping Retry Timer (milliseconds)*	500
Ping Retry Count*	6

Create SIP Trunk Security Profile.

Use the System > Security > SIP Trunk Security Profile menu option in Cisco Unified Communications Manager Administration to create SIP Trunk Security profile for recorder.

- Set Incoming Transport Type to TCP+UDP.
- Set Outgoing Transport Type to TCP.
- Uncheck option Enable Digest Authentication



SIP Trunk Security Profile Information

Name*	teliscaAgent SIP Trunk Security Profile
Description	teliscaAgent SIP Trunk Security Profile
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5060
□ Enable Application level authorization	
□ Accept presence subscription	
□ Accept out-of-dialog refer**	
□ Accept unsolicited notification	
□ Accept replaces header	
□ Transmit security status	
□ Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

- Set Device Security Mode parameter to Non-Secure.

Create a SIP Trunk That Points to the Recorder

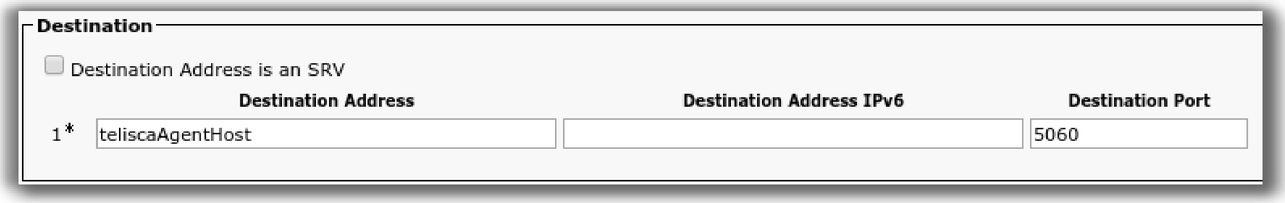
Enter the recorder DN, which must match a route pattern for the SIP trunk or a route list that includes the recorder.

Choose the appropriate SIP profile and SIP Trunk Security Profile that you configured for recording.

Use the Device > Trunk menu option in Cisco Unified Communications Manager Administration to perform the following configuration:

Destination Address: telisca recording agent host.

Destination Port: telisca recording agent SIP trunk signaling port, default is 5060.



Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	teliscaAgentHost		5060

Create a Route Pattern for the Recorder

Create a route pattern for the recorder SIP trunk. The Recording Destination Address in the recording profile must match this pattern.

Select the SIP trunk that points to the recorder, or select a route list of which the recorder is a member.

Use the Call Routing > Route/Hunt > Route Pattern menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Create Recorder Redundancy

You can also use the following mechanism to achieve recorder redundancy:

- Use the SRV record for the recorder destination address in SIP trunk configuration.
- Use multiple recorders for redundancy and load balance. Create a SIP trunk for each recorder; create a route list to include the route groups that have individual SIP trunks as a member.

Use the Device > Trunk menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Recording Server Redundancy

The redundancy with telisca Recording is supported by using a **Route List approach**.

- Configure two SIP trunks for each addressable recorder or recorder proxy.
- Assign your SIP trunks to a recorder route group with an assigned algorithm. The algorithm needs to be top down.
- Assign the recorder route group to a route list.
- Use a route pattern to direct traffic to the recorder route list.

Limit Codec Usage for Recording Calls

Because the codecs for recording calls match the codecs for agent-customer calls, you may need to insert transcoders if the recorder does not support the matching codecs.

Cisco Unified IP Phones adds new codecs that Cisco transcoders do not support.

Use the following service parameters to enable or disable usage of the G722, iLBC, and iSAC codecs:

G722 Codec Enabled or Disabled

iLBC Codec **Disabled** (telisca recording Agent do not support)

iSAC Codec **Disabled** (telisca recording Agent do not support)

Find these service parameters in the Clusterwide Parameters (System - Location and Region) section of the Service Parameter Configuration window.

You can set these service parameters with the following values:

- Enabled for All Devices
- Enabled for All Devices Except Recording-Enabled Devices
- Disabled

6.2 Set up CUCM to upload CDR to telisca Recording Manager

- Connect Cisco Unified Serviceability console.
- Choose Tools > CDR Management Configuration. The CDR Management Configuration window displays.
- Perform one of the following tasks:

  To add a new application billing server, click the Add New button.

  To update an existing application billing server, click the server hostname/IP address.

- Enter the application billing server parameter settings.
- Click Add or Update.

Then use the following parameters to configure the server:

- Host Name/IP Address: telisca Recording Manager Host Name or IP Address.
- User Name: SFTP login.
- Protocol: SFTP
- Directory Path: Have to include internal CUCM name from CUCM/Server configuration (ex : /CUCM_INTERNAL_NAME/).
- Password: SFTP password.
- Resend on Failure: yes.

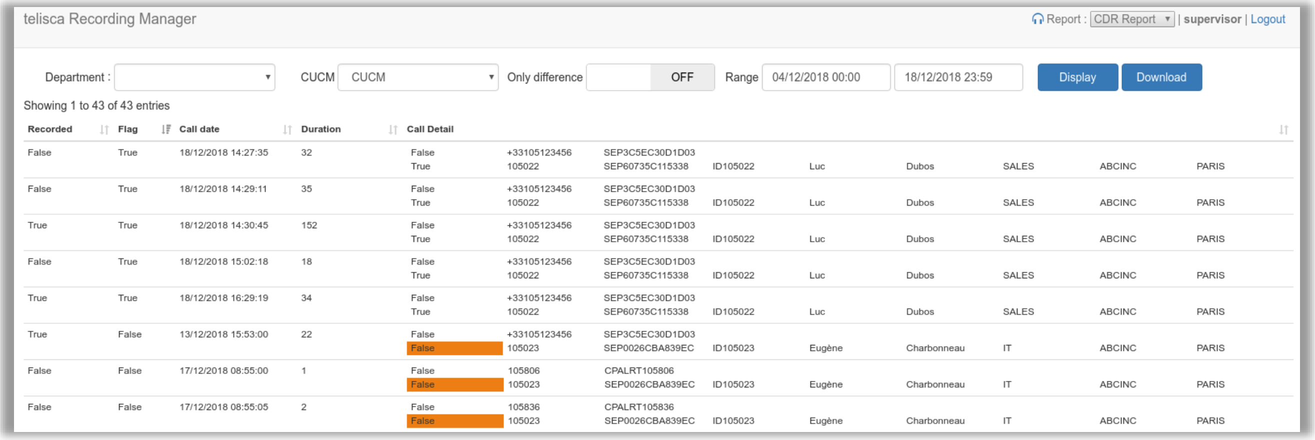
7 Reports

7.1 CDR report

An execution report allows to compare telisca recording Agents records to CUCM CDR call history data for recorded lines.

- Orange flag – recording option is automatic and recording profile is set but the line's required flag not set.

- Red flag – recording option is not automatic or recording profile is missing but the line's required flag set.



telisca Recording Manager

Report : CDR Report ▾ | **supervisor** | Logout

Department : ▾ CUCM CUCM ▾ Only difference OFF Range 04/12/2018 00:00 18/12/2018 23:59 Display Download

Showing 1 to 43 of 43 entries

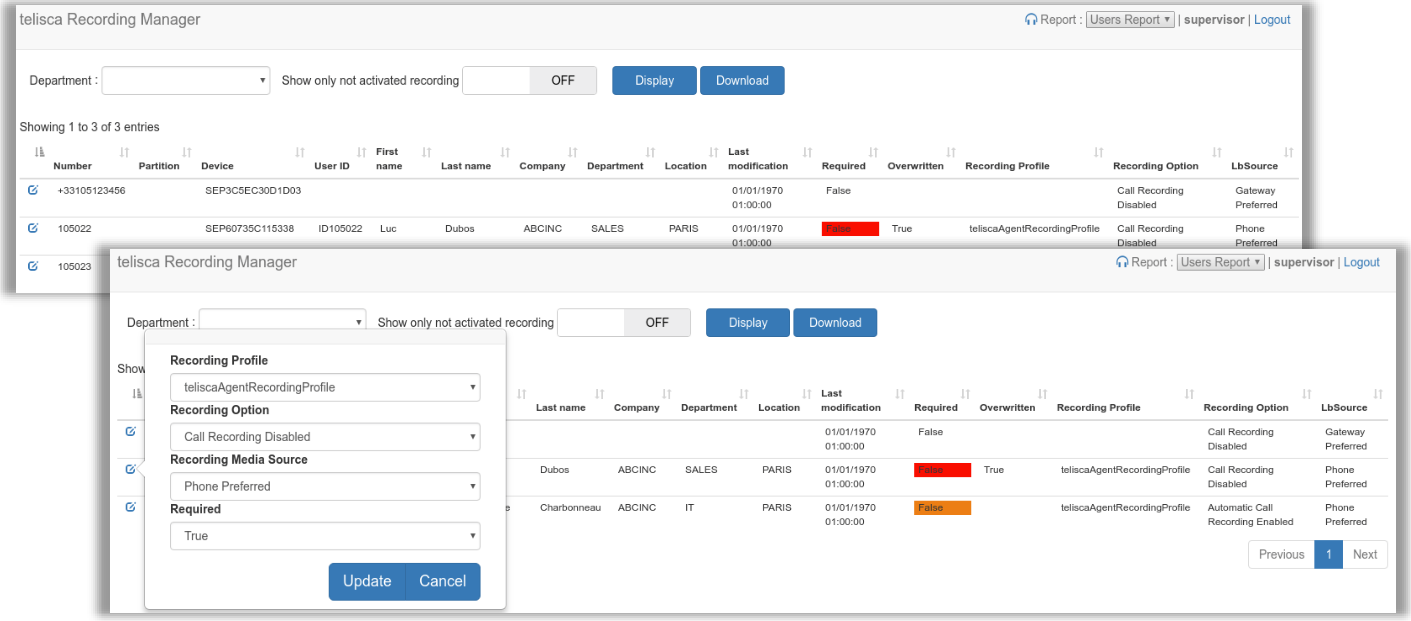
Recorded	Flag	Call date	Duration	Call Detail								
False	True	18/12/2018 14:27:35	32	False True	+33105123456 105022	SEP3C5EC30D1D03 SEP60735C115338	ID105022	Luc	Dubos	SALES	ABCINC	PARIS
False	True	18/12/2018 14:29:11	35	False True	+33105123456 105022	SEP3C5EC30D1D03 SEP60735C115338	ID105022	Luc	Dubos	SALES	ABCINC	PARIS
True	True	18/12/2018 14:30:45	152	False True	+33105123456 105022	SEP3C5EC30D1D03 SEP60735C115338	ID105022	Luc	Dubos	SALES	ABCINC	PARIS
False	True	18/12/2018 15:02:18	18	False True	+33105123456 105022	SEP3C5EC30D1D03 SEP60735C115338	ID105022	Luc	Dubos	SALES	ABCINC	PARIS
True	True	18/12/2018 16:29:19	34	False True	+33105123456 105022	SEP3C5EC30D1D03 SEP60735C115338	ID105022	Luc	Dubos	SALES	ABCINC	PARIS
True	False	13/12/2018 15:53:00	22	False False	+33105123456 105023	SEP3C5EC30D1D03 SEP0026CBA839EC	ID105023	Eugène	Charbonneau	IT	ABCINC	PARIS
False	False	17/12/2018 08:55:00	1	False False	105806 105023	CPALRT105806 SEP0026CBA839EC	ID105023	Eugène	Charbonneau	IT	ABCINC	PARIS
False	False	17/12/2018 08:55:05	2	False False	105836 105023	CPALRT105836 SEP0026CBA839EC	ID105023	Eugène	Charbonneau	IT	ABCINC	PARIS

7.2 User report

A report allows the review the status and update the recording profile and recording option of CUCM in case of BIB recording, also possible to overwrite internal require flag.

- Yellow flag – line does not exist in CUCM.

- Red flag – recording option is not automatic or recording profile is missing but the line requires flag set.



telisca Recording Manager

Report : Users Report ▾ | **supervisor** | Logout

Department : ▾ Show only not activated recording OFF Display Download

Showing 1 to 3 of 3 entries

	Number	Partition	Device	User ID	First name	Last name	Company	Department	Location	Last modification	Required	Overwritten	Recording Profile	Recording Option	LbSource
✎	+33105123456		SEP3C5EC30D1D03							01/01/1970 01:00:00	False			Call Recording Disabled	Gateway Preferred
✎	105022		SEP60735C115338	ID105022	Luc	Dubos	ABCINC	SALES	PARIS	01/01/1970 01:00:00	False	True	teliscaAgentRecordingProfile	Call Recording Disabled	Phone Preferred
✎	105023														

telisca Recording Manager

Report : Users Report ▾ | **supervisor** | Logout

Department : ▾ Show only not activated recording OFF Display Download

Recording Profile: teliscaAgentRecordingProfile ▾

Recording Option: Call Recording Disabled ▾

Recording Media Source: Phone Preferred ▾

Required: True ▾

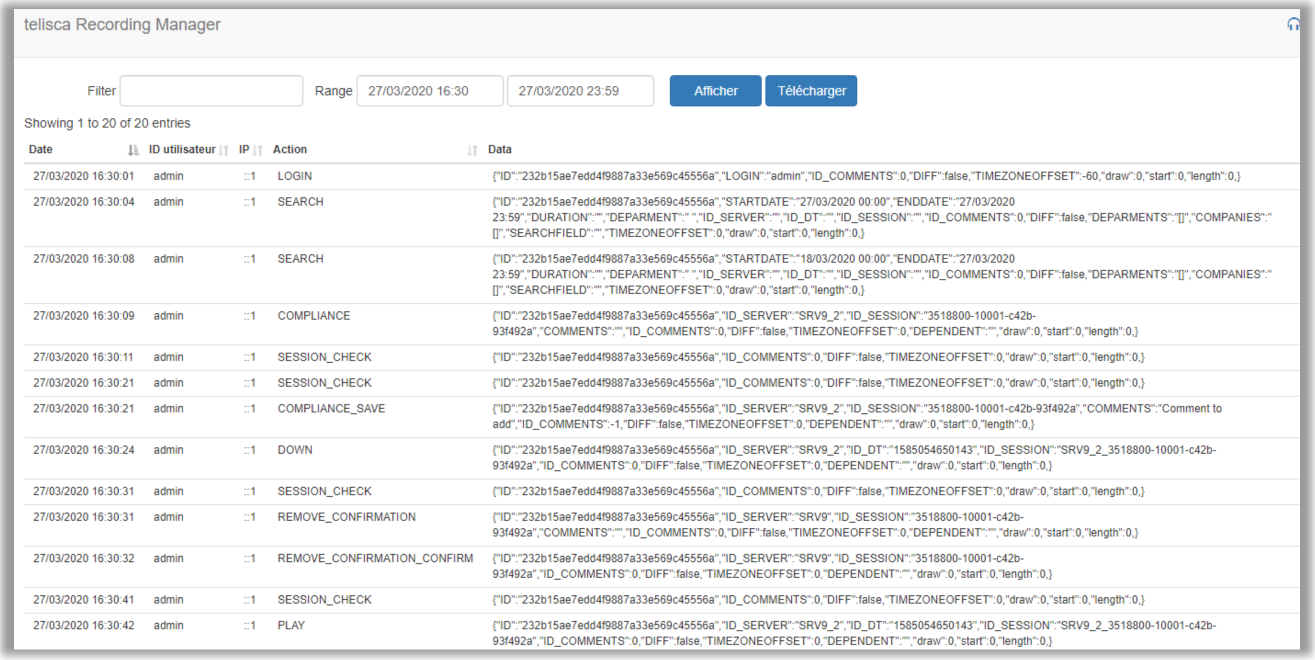
Update Cancel

	Last name	Company	Department	Location	Last modification	Required	Overwritten	Recording Profile	Recording Option	LbSource
✎					01/01/1970 01:00:00	False			Call Recording Disabled	Gateway Preferred
✎	Dubos	ABCINC	SALES	PARIS	01/01/1970 01:00:00	False	True	teliscaAgentRecordingProfile	Call Recording Disabled	Phone Preferred
✎	Charbonneau	ABCINC	IT	PARIS	01/01/1970 01:00:00	False		teliscaAgentRecordingProfile	Automatic Call Recording Enabled	Phone Preferred

Previous 1 Next

7.3 Actions Log

The report allows you review all user interaction with application, such as LOGIN, SEARCH, DOWN (download), PLAY, REMOVE, etc. The application keeps historical data for 1825 days.



Range 27/03/2020 16:30 – 27/03/2020 23:59

Showing 1 to 20 of 20 entries

Date	ID utilisateur	IP	Action	Data
27/03/2020 16:30:01	admin	::1	LOGIN	{"ID":"232b15ae7edd4f9887a33e569c45556a","LOGIN":"admin","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":-60,"draw":0,"start":0,"length":0,}
27/03/2020 16:30:04	admin	::1	SEARCH	{"ID":"232b15ae7edd4f9887a33e569c45556a","STARTDATE":"27/03/2020 00:00","ENDDATE":"27/03/2020 23:59","DURATION":"","DEPARMENT":" ","ID_SERVER":"","ID_DT":"","ID_SESSION":"","ID_COMMENTS":0,"DIFF":false,"DEPARMENTS":"[]","COMPANIES":"[]","SEARCHFIELD":"","TIMEZONEOFFSET":0,"draw":0,"start":0,"length":0,}
27/03/2020 16:30:08	admin	::1	SEARCH	{"ID":"232b15ae7edd4f9887a33e569c45556a","STARTDATE":"18/03/2020 00:00","ENDDATE":"27/03/2020 23:59","DURATION":"","DEPARMENT":" ","ID_SERVER":"","ID_DT":"","ID_SESSION":"","ID_COMMENTS":0,"DIFF":false,"DEPARMENTS":"[]","COMPANIES":"[]","SEARCHFIELD":"","TIMEZONEOFFSET":0,"draw":0,"start":0,"length":0,}
27/03/2020 16:30:09	admin	::1	COMPLIANCE	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_SERVER":"SRV9_2","ID_SESSION":"3518800-10001-c42b-93f492a","COMMENTS":"","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"DEPENDENT":"","draw":0,"start":0,"length":0,}
27/03/2020 16:30:11	admin	::1	SESSION_CHECK	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"draw":0,"start":0,"length":0,}
27/03/2020 16:30:21	admin	::1	SESSION_CHECK	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"draw":0,"start":0,"length":0,}
27/03/2020 16:30:21	admin	::1	COMPLIANCE_SAVE	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_SERVER":"SRV9_2","ID_SESSION":"3518800-10001-c42b-93f492a","COMMENTS":"Comment to add","ID_COMMENTS":-1,"DIFF":false,"TIMEZONEOFFSET":0,"DEPENDENT":"","draw":0,"start":0,"length":0,}
27/03/2020 16:30:24	admin	::1	DOWN	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_SERVER":"SRV9_2","ID_DT":"1585054650143","ID_SESSION":"SRV9_2_3518800-10001-c42b-93f492a","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"DEPENDENT":"","draw":0,"start":0,"length":0,}
27/03/2020 16:30:31	admin	::1	SESSION_CHECK	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"draw":0,"start":0,"length":0,}
27/03/2020 16:30:31	admin	::1	REMOVE_CONFIRMATION	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_SERVER":"SRV9","ID_SESSION":"3518800-10001-c42b-93f492a","COMMENTS":"","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"DEPENDENT":"","draw":0,"start":0,"length":0,}
27/03/2020 16:30:32	admin	::1	REMOVE_CONFIRMATION_CONFIRM	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_SERVER":"SRV9","ID_SESSION":"3518800-10001-c42b-93f492a","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"DEPENDENT":"","draw":0,"start":0,"length":0,}
27/03/2020 16:30:41	admin	::1	SESSION_CHECK	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"draw":0,"start":0,"length":0,}
27/03/2020 16:30:42	admin	::1	PLAY	{"ID":"232b15ae7edd4f9887a33e569c45556a","ID_SERVER":"SRV9_2","ID_DT":"1585054650143","ID_SESSION":"SRV9_2_3518800-10001-c42b-93f492a","ID_COMMENTS":0,"DIFF":false,"TIMEZONEOFFSET":0,"DEPENDENT":"","draw":0,"start":0,"length":0,}

8 Cisco Finesse Gadgets

8.1 Desktop configuration

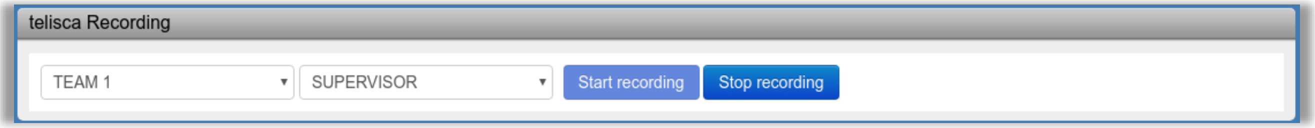
Connect the Finesse administration by going to: https://<FQDN>:8445/cfadmin/ , where FQDN is the fully qualified domain name of the Finesse server

If your team's are utilizing the default layout, Click on the desktop layout tab. Otherwise, click on the Team Resources tab to edit a specific team's layout add the following lines, where FQDN is the fully qualified domain name of the telisca recording manager server and PORT is web interface port:

For telisca recording start/stop gadget:

```
<gadgets>
        <gadget> https://<FQDN>:<PORT>/gadgets/trg/trg.xml</gadget>
</gadget>
```

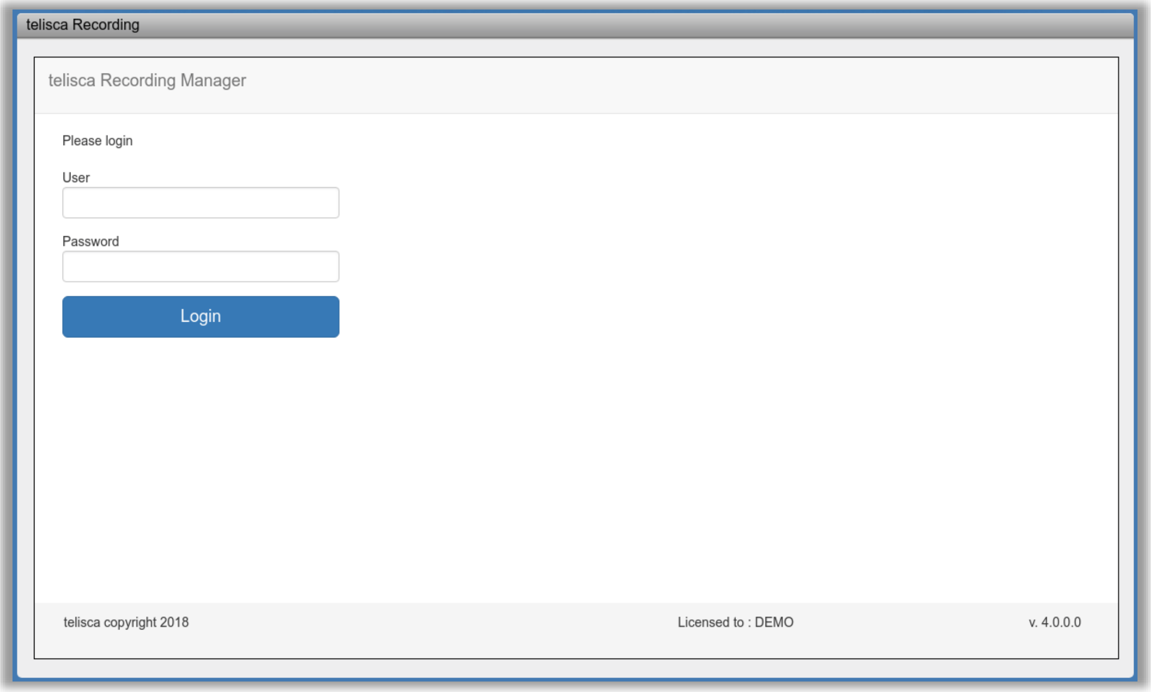
This gadget allows you start and stop current agent recording or any agent of team in case of supervisor.



For telisca recording interface gadget:

```
<gadgets>
        <gadget> https://<FQDN>:<PORT>/gadgets/ewa/ewa.xml</gadget>
</gadgets>
```

This gadget allows you assess to telisca recording web interface as a gadget.



The Finesse server caches all gadgets. If updates are made to a gadget either the Finesse Tomcat service must be restarted (not recommended during production) or the ?nocache flag can be added to the end of the Finesse URL in the browser. For example (where FQDN is the fully qualified domain name of the Finesse server):

https://<FQDN>:8445/desktop/container/?nocache.

The '?nocache' flag forces a new version of the gadget to be loaded. After 24 hours Tomcat will automatically update its cached gadgets as well.

8.2 Add Certificate for HTTPS Gadget

Add a certificate for a secure HTTP (HTTPS) allow the gadget to load into the Finesse desktop and successfully perform HTTPS requests to the Finesse server.

This process allows HTTPS communication between the Finesse gadget container and the telisca server for loading the gadget and performing any API calls that the gadget makes to the telisca server.

The Finesse host must be able to resolve this name using the DNS host that was entered during installation. To verify that Finesse can resolve the name, run the CLI command "utils network ping <host-name>".

Step 1

Download the trm_cert.cer certificate from 'Drive where the application installed'\TRM\CERT\.

Step 2

Upload the certificate to the primary Finesse server.

Sign in to Cisco Unified Operating System Administration on the primary Finesse server (http://FQDN:8443/cmplatform, where FQDN is the fully qualified domain name of the Finesse server).

Click Security > Certificate Management.

Click Upload Certificate.

From the Certificate Name drop-down list, select tomcat-trust.

Click Browse and navigate to the trm_cert.cer file that you downloaded in the previous step.

Click Upload File.

Step 3

Restart Cisco Finesse Tomcat on the primary Finesse server.

Step 4

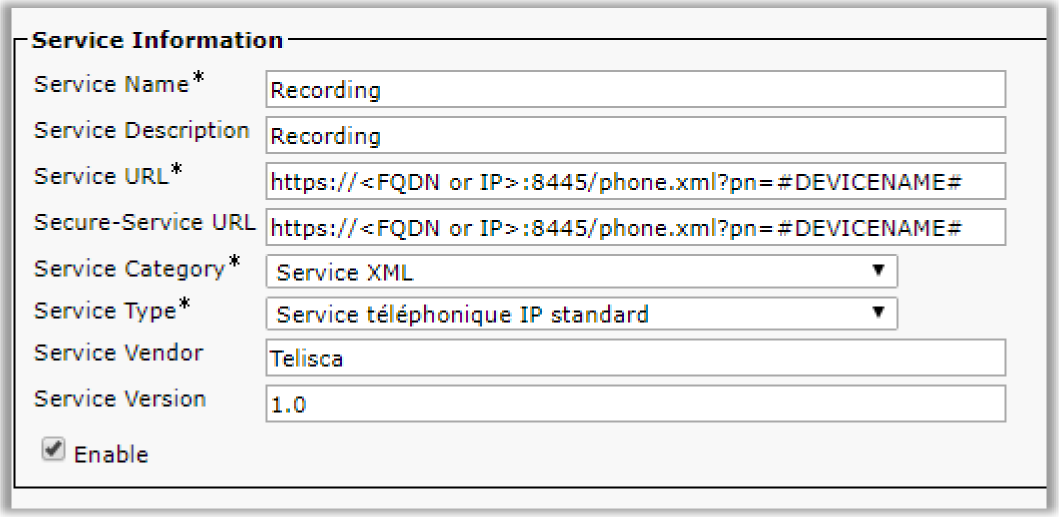
After synchronization is complete, restart Cisco Finesse Tomcat on the secondary Finesse server.

9 Recording IP Phone Services

9.1 CUCM configuration

The IP Phone Services allows you to start, stop current recording. Also, the recording cab be marked for deletion or to keep for exception duration.

The IP Phone Services URL is following: https://<FQDN or IP>:8445/phone.xml?pn=#DEVICE-NAME# , where FQDN (fully qualified domain name) or IP is the of the telisca server



Service Information

Service Name*	Recording
Service Description	Recording
Service URL*	https://<FQDN or IP>:8445/phone.xml?pn=#DEVICENAME#
Secure-Service URL	https://<FQDN or IP>:8445/phone.xml?pn=#DEVICENAME#
Service Category*	Service XML
Service Type*	Service téléphonique IP standard
Service Vendor	Telisca
Service Version	1.0

☑ Enable

The AGENT_ACTION parameter can be used to delete or keep action on current recording without main application screen.

https://<FQDN or IP>:8445/phone.xml?pn=#DEVICENAME#&AGENT_ACTION=DELETE
or
https://<FQDN or IP>:8445/phone.xml?pn=#DEVICENAME#&AGENT_ACTION=KEEP

9.2 Add Certificate on CUCM for HTTPS communication

Add a certificate for a secure HTTP (HTTPS) allow the service to load into the phone and successfully perform HTTPS requests to the telisca server.

Step 1

Download the trm_cert.cer certificate from 'Drive where the application installed'\TRM\CERT\.

Step 2

Upload the certificate to the CUCM server.

The certificate has to be uploaded to CUCM under the OS Administration page > Security > Certificate Management.

Upload it as a "Tomcat-Trust".

Step 3

Restart Cisco Tomcat on the CUCM server. Could be done also by command line 'utils service restart Cisco Tomcat'

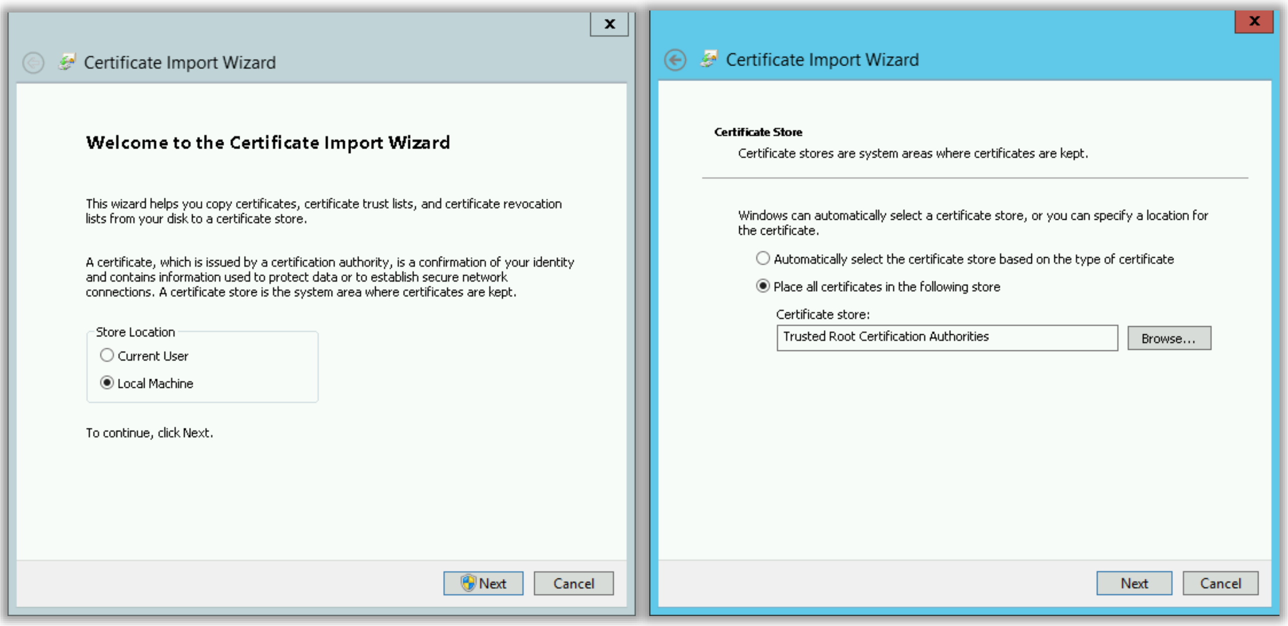
10 TRM Certificate replacement

Following procedure can be used to replace self-signed certificate installed during initial application setup.

New certificate has to has the private key.

Step 1 Install new certificate.

Install new certificate on server with following parameters: store location: ‘Local Machine’, certificate store: ‘Trusted Root Certification Authorities’.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate
● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Step 2 Get a certificate's thumbprint.

Use the Certificates MMC snap-in to find an X.509 certificate that has an intended purpose of client authentication

Access the certificate's thumbprint. Copy the thumbprint of the certificate into a text editor, such as Notepad. Remove all spaces between the hexadecimal characters. One way to accomplish this is to use the text editor's find-and-replace feature and replace each space with a null character.

Step 3 Delete an SSL certificate from a port number (Command prompt with administrator rights).

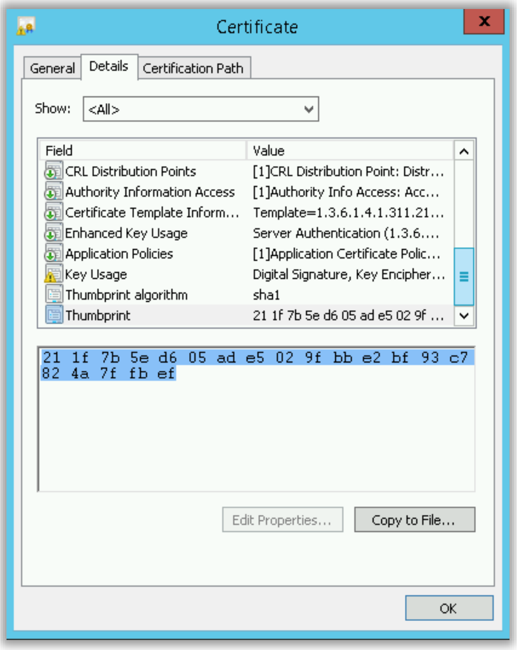
```
netsh http delete sslcert 0.0.0.0:8445
```

Before this step you can copy current certificate’s, thumbprint using:

```
netsh http show sslcert ipport=0.0.0.0:8445
```

Step 4 Bind an SSL certificate to a port number. (Command prompt with administrator rights).

```
netsh http add sslcert ipport=0.0.0.0:8445 certhash=NEW_THUMBPRINT appid={377b2c7c-c3e8-4ed7-abe5-83816b8ec353} certstorename=Root
```



Certificate

Show: <All>

Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr…
Authority Information Access	[1]Authority Info Access: Acc…
Certificate Template Inform…	Template=1.3.6.1.4.1.311.21…
Enhanced Key Usage	Server Authentication (1.3.6.…
Application Policies	[1]Application Certificate Polic…
Key Usage	Digital Signature, Key Encipher…
Thumbprint algorithm	sha1
Thumbprint	21 1f 7b 5e d6 05 ad e5 02 9f …

```
21 1f 7b 5e d6 05 ad e5 02 9f bb e2 bf 93 c7
82 4a 7f fb ef
```

11 Troubleshooting

telisca Recording solution has multiple components.

Here where you can find the logs, configuration files and internal DB backup (in case of use internal PostgreSQL PostgreSQL DB).

telisca Recording Manager

Service name: telisca RM Service

Log files location: 'Drive where the application installed'\TRM\LOGS\

Log files format: TRM_yyMMddHh.X.log

Log files web server format: TRM_HTTP_yyMMddHh.X.log

Data files location: 'Drive where the application installed'\TRM\DATA\

DB backup location (if DB backup is configured in 5.6 Parameters): 'Drive where the application installed'\TRM\BACKUP\

telisca Recording Agent

Service name: telisca RA Service

Log files location: 'Drive where the application installed'\TRM\LOGS\

Log files format: TRA_yyMMddHh.X.log

Log files web server format: TRM_HTTP_yyMMddHh.X.log

Data files location: 'Drive where the application installed'\TRM\DATA\

PostgreSQL

Service name: PostgreSQL for TRM

Log files location: 'Drive where the application installed'\PG\DB\log\

Log files format: postgresql-yyyy-MM-dd_Hmmss.log