Product Datasheet

telisca Microsoft Teams 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

1 Solution description

1.1 Summary

The telisca Microsoft Teams Recording solution is based on a Recording Manager and one or several Recording Agents.

telisca recording Agent for MS Teams:

- Support audio recording of all type of the calls
- Support pause, resume
- Calls converts to MP3
- Support consult, transfer, conference calls
- Support fault tolerant configuration

telisca Recording Manager :

- Archive recordings on efficient network storage
- Encrypt recordings
- Automatic purge depending of retention delay (per department/company)
- Annotation of recordings with information provided by the company's internal directory, which can be loaded up by Azure AD or CSV
- Authentication/segmentation of users by Azure AD
- Web interface for searching recordings by last name, first name, location, with contacts segmented and filtered by department/company
- Listen to streamed recordings via a web interface, with option to download recording
- Add notes while listening
- Optionally user can browse and listen its' own recordings
- History of recordings which have been reviewed (date, compliance officer, comments, …)

1.2 Feature details

1.2.1 Archiving

Recordings are periodically transcoded and stored on network storages, which may be on separate storage devices as determined by the organization of the enterprise. It is possible to define a separate storage device for each recording Agent, as well as by department/company.

It is possible to use a local temporary storage before exporting to network storage. Export from the Recording Agent and to the network storages can be executed during specific time range to save the network bandwidth during working hours.

1.2.2 Audio file encryption option

Optionally, it is possible to encrypt the audio files after their export and conversion to MP3 on the secured shared network storage.

1.2.3 Recording database

At the same time that the recordings are exported, meta data recorded by the Recording Agent are retrieved and enriched in the Recording Manager's database, with information obtained from Azure Active Directory or from a text file.

Directory contacts are retrieved by telephone number or by userId of the caller or the called party. The information stored includes: userId, last name, first name, department, company, location, comment, ….

1.2.4 Web interface user authentication and segmentation

Access to the web interface (https) to search and listen recordings is controlled by authentication based upon an Azure Active Directory login.

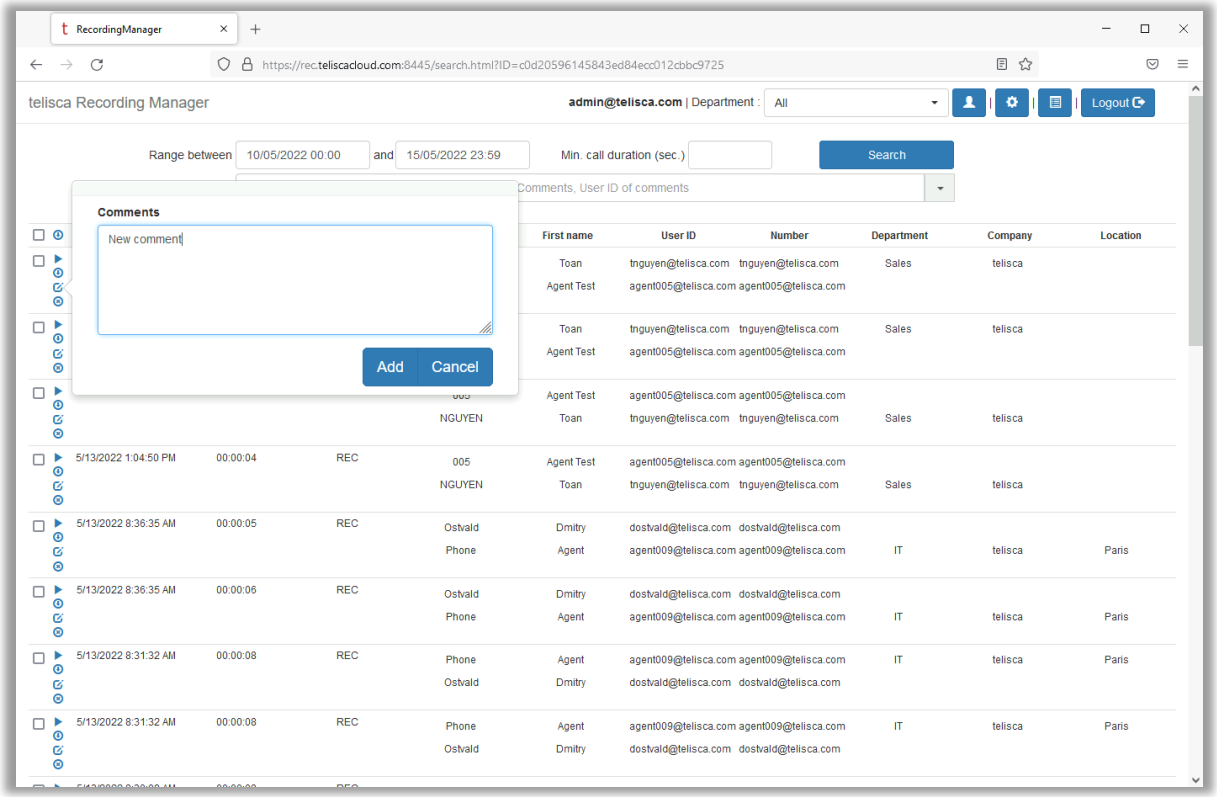
The user can be authorized to listen his own recording. The supervisor can listen recording from selected companies/departments.

Authorization and segmentation can be defined in Azure Active Directory.

- The supervisor must be part of one or several security user groups associated with a department's attribute. The supervisor will be authorized to search and listen the recordings of the agents of the defined departments.

1.2.5 Database search, listen to recordings

Users who are authorized to search recordings for a selected entity may search by: userID, Last name, first name, telephone number, date / time range, call duration, department/company, comment.



The information available in the replicated database is displayed in a search results grid. When clicking on an icon, the recording may be listened via streaming or, optionally, may be downloaded (with a specific authorization level). Comments can be added. The recording can be marked for immediate Purge or increased retention.

1.2.6 Database purge

Depending upon retention parameters, database search results will be filtered, excluding those results whose age exceeds the retention limit. In addition, a physical purge of files is automatically effected.

Different retention parameters can be defined depending of the company/department.

1.3 Architecture, prerequisites

1.3.1 Recording Manager

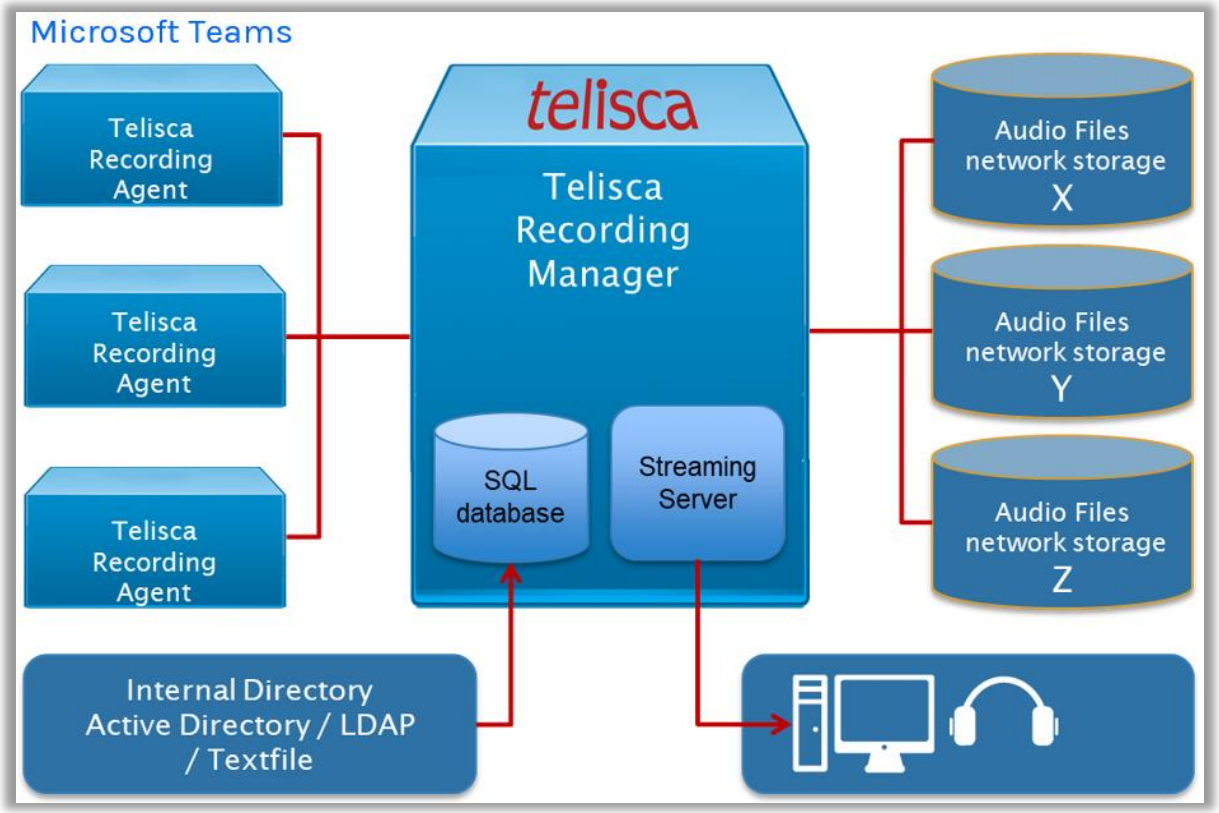
The telisca Recording Manager is installed on a Windows (on premise or on cloud), which may be virtualized and may be co-located with other telisca applications.

The audio files obtained from one or several Recording Agents are periodically converted to MP3 format, on a safeguarded storage device. The volume of stored MP3 files is approximately 500 kilobytes per minute of recording.

It is possible to define timeframes (by department/company) for exporting and copying the audio files in order to minimize bandwidth requirements during busy periods.

The server relies on an SQL database which may be synchronized in fault tolerance. Microsoft SQL Server Standard and PostgreSQL (freeware) are supported.

The application includes an, HTML5 compatible, audio streaming server,.



Access to recordings is via an HTML5 compatible browser, in HTTPS, and is subject to authentication.

Available on private cloud company.telisca.cloud

On premise or cloud installation:

Windows servers supported:

- Windows Server 2012 R2 v6.3 (Build 9600) Essentials or Standard
- Windows Server 2016 Essentials or Standard
- Windows Server 2019 Essentials or Standard
- Windows Server 2022 Standard

Hardware configuration:

- Minimum configuration: 1 vCPU, 4GB RAM, 100GB disk
- + 8 GB/agent/year archiving
- Virtual Machine VMware vSphere, Hyper-V
- PostgreSQL v14.x (installed by Setup) or Microsoft SQL Server Standard 2012, 2014, 2016, 2019 & 2022.

Browsers supported:

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

1.3.2 Recording Agent for MS Teams

Supported Servers OS and requirements:

- Windows Server 2012 R2 v6.3 (Build 9600) Essentials or Standard
- Windows Server 2016 Essentials or Standard
- Windows Server 2019 Essentials or Standard
- Windows Server 2022 Standard

- Microsoft requires that the Recording agent be in Azure.

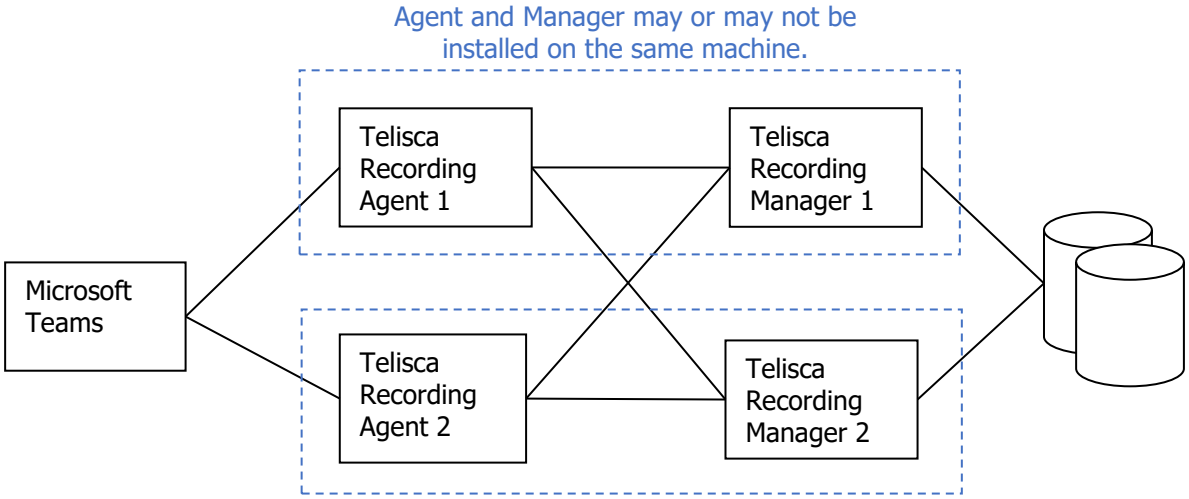
- VM hosting a Recording agent must have a public IP and a CNAME record that belongs to the domain that is pointing to this public IP address.

Minimum hardware configuration needed by application:

- Standard_DS3_v2 - 100 calls
- Standard_DS4_v2 - 200 calls
- Standard_DS5_v2 - 400 calls

1.3.3 Optionnal fault tolerance module

The optional fault tolerant configuration allows to continue recording the calls when the main server is down.



This mode requires registering two bots. The two bots are registered under the same Microsoft tenant.

The telisca Recording Manager may also be duplicated and will execute in Active/Active mode. Configurations are synchronized through the SQL database that need to be secured (cluster mode).

To offer a seamless access to Recording Manager's Web interface, a Virtual IP address or DNS can be configured using an external Load Balancer or Windows Network Load Balancer.